MISSISSIPPI LAW JOURNAL

SYMPOSIUM

PROSECUTION RESPONSES TO INTERNET VICTIMIZATION

SPONSORED BY THE
NATIONAL CENTER FOR JUSTICE AND THE RULE OF LAW

FOREWORD
Thomas K. Clancy

KEYNOTE ADDRESS: PROSECUTION RESPONSES TO INTERNET VICTIMIZATION
The Honorable M. Jane Brady

INTERNET AND COMPUTER RELATED CRIME: ECONOMIC AND OTHER HARMS TO ORGANIZATIONAL ENTITIES
Edward M. Roche

TECHNOLOGY, STALKING AND DOMESTIC VIOLENCE VICTIMS
Cindy Southworth and Sarah Tucker

CHILD PORNOGRAPHY AND FIRST AMENDMENT STANDARDS
Kyle Duncan

SHOULD ONLINE DEFAMATION BE CRIMINALIZED?
Susan W. Brenner

PANEL DISCUSSION I: THE DECISION TO PROSECUTE

PANEL DISCUSSION II: PREPARING THE CASE AFTER THE DECISION TO PROSECUTE HAS BEEN MADE

PROSECUTING THE INTERNET FRAUD CASE WITHOUT GOING BROKE
Patrick E. Corbett

PANEL DISCUSSION III: WORKING WITH CORPORATIONS ON CASE INVESTIGATIONS

SENTENCING POLICY AND PROCEDURE AS APPLIED TO CYBER CRIMES: A CALL FOR RECONSIDERATION AND DIALOGUE
Donald R. Mason

INTERNET CRIME VICTIMIZATION: SENTENCING
John F. Curran

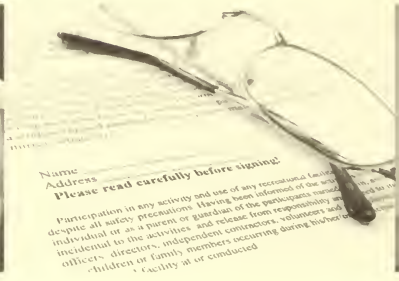
THINKING THROUGH SENTENCING IN COMPUTER HACKING CASES: DID THE U.S. SENTENCING COMMISSION GET IT RIGHT?
Richard W. Downing

CREATIVE SANCTIONS FOR ONLINE INVESTMENT FRAUD
Jayne W. Barnard

VOLUME 76 **WINTER 2007** **NUMBER 3**

MISSISSIPPI BRIEFING SERVICE

...an indispensable service provided by the... MISSISSIPPI LAW JOURNAL



In the legal world, timely and accurate ***communication*** *is a key to* ***success...***

How can you stay informed of the latest appellate decisions without sacrificing your valuable time?

Answer: the Mississippi Briefing Service

Each week, *Recent Decisions of the Mississippi Supreme Court and Court of Appeals* briefs the latest opinions of the Courts. In addition to concise and accurate summaries, each case is supplemented with appropriate and accurate headnotes—which means you find the cases you need and only the cases you need.

Annual subscription to the Mississippi Briefing Service is available for $85 and is provided in searchable, electronic format via e-mail, providing you the information you need even faster.

To subscribe, or for a free sample brief:

- e-mail: MSBRIEF@OLEMISS.EDU
- write: MISSISSIPPI LAW JOURNAL
  P.O. Box 849
  University, Mississippi 38677

MISSISSIPPI LAW JOURNAL
student-operated, student-lead, practitioner-focused

Give yourself the advantage of experience

When you need business valuation, forensic accounting or litigation support services, look carefully for professionals who have the credentials, expertise and — most important — the experience required to deliver timely, accurate and reliable service.

At Grantham Poole CPAs, we have what you're looking for. Over the past 30 years, our firm has built a strong reputation for providing solutions that make our clients' lives easier and more profitable. We offer first-class business valuation and litigation support services for a broad range of purposes, including:

- ☑ Shareholder disputes
- ☑ Estate planning and settlement
- ☑ Buy/sell agreements
- ☑ Marital dissolutions
- ☑ Business interruptions
- ☑ Calculation of lost profits
- ☑ Determination of actual and punitive damages
- ☑ Fraud investigations
- ☑ Courtroom testimony
- ☑ Mediation and arbitration
- ☑ Financial data analysis
- ☑ Business sales, mergers and acquisitions

Our highly skilled and experienced professionals hold a variety of relevant credentials, including Certified Public Accountant (CPA), Accredited in Business Valuation (ABV), Certified Valuation Analyst (CVA), Certified Financial Planner (CFP) and Certified Fraud Examiner (CFE).

Everyone in our firm is dedicated to serving our clients and our community with trust, integrity and excellence. We don't just respond to your requests. We proactively anticipate your needs and suggest solutions that give you an advantage, both in and out of court.

Our skilled valuation and litigation support team is eager to help you achieve your objectives:

Stephanie B. Smith, CPA

Robert A. Cunningham, CPA, CFE, CVA

Charles P. Rafferty, CPA, CFE, CVA

J. Thomas Grantham, Jr., CPA, CFP, ABV

George W. Butler, Jr., CPA

James E. Poole, CPA

R. Vance Randall, CPA

We welcome the opportunity to discuss your needs and put our knowledge and experience to work for you. Please call us at 601-957-5050 and let us know how we can be of assistance. ✧

Grantham, Poole, Randall, Reitano, Arrington, & Cunningham, PLLC
Certified Public Accountants

Trusted advisors, solving your problems

Robert C. Khayat Scholarship Endowment

The *Mississippi Law Journal* established the endowment in February of 1995 to honor the dedicated service of Robert C. Khayat, former Law Journal member, professor and current University Chancellor. The purpose of the endowment is to assist distinguished men and women of the *Journal* in the pursuit of their legal education at the University of Mississippi. As of June 30, 2006, the corpus of the endowment was $60,935.37. Each year deserving *Journal* members are awarded scholarships as selected by the Executive Board of the *Journal*. This year $1,000 was awarded to Journal members. Please help us increase the corpus of the endowment so that we can increase the number and size of these scholarships.

Checks should be made payable to and mailed to:

The University of Mississippi Foundation
Post Office Box 8288
University, MS 38677

Please note on your check that your gift is designated for the Robert C. Khayat Scholarship Endowment.

Contributions are tax deductible.

The *Mississippi Law Journal* is published four times during the school year, including a Special Edition. Editorial and business offices: Post Office Box 849, University, Mississippi 38677.

Current subscription: $35.00 per year. Single issue: $12.00. Subscriptions are renewed automatically upon expiration unless the subscriber sends a notice of termination.

Change of address: Send address changes directly to the *Mississippi Law Journal*. Include name, new address (including zip code) and old address. Please notify the *Journal* forty-five days in advance to ensure prompt delivery. Unless a claim is made for nonreceipt of the *Journal* within six months after the mailing date, the *Mississippi Law Journal* cannot be held responsible for supplying those issues without charge. Third class postage paid at University, Mississippi 38677 and additional mailing offices.

Manuscripts should be submitted electronically to **misslj@olemiss.edu**. Contributors are requested to submit articles in 12-point type and double-spaced, in Microsoft Word, WordPerfect, or PDF. Citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (18th ed. 2005).

The *Mississippi Law Journal* is a member of the National Conference of Law Reviews.

To offer its contributors complete freedom, the *Journal* assumes no responsibility for the views expressed herein.

Back issues of the *Mississippi Law Journal* may be ordered directly from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York 14029-1987. Orders may also be placed by calling William S. Hein & Co., Inc. at (800) 828-7571, via fax at (716) 883-8100 or email to order@wshein.com. Back issues are also available in PDF format through HeinOnline.

Administrative Officers of the University of Mississippi

Robert C. Khayat	*Chancellor*
Carolyn Ellis Staton	*Provost and Vice Chancellor for Academic Affairs*
Gloria Kellum	*Vice Chancellor for University Affairs*
Alice Clark	*Vice Chancellor for Research and Sponsored Programs*
Johnny Williams	*Vice Chancellor for Administration and Finance*
Wendell Weakley	*President/CEO, The University of Mississippi Foundation*
Timothy L. Hall	*Associate Provost*
Thomas Wallace	*Vice Chancellor for Student Life*
Andrew P. Mullins, Jr.	*Executive Assistant to the Chancellor*
Timothy L. Walsh	*Associate Dean for Development*
Samuel M. Davis	*Dean of the School of Law, Director of Law Center, Jamie L. Whitten Chair of Law and Government and Professor of Law*

The Law School Faculty

Guthrie T. Abbott, *Professor Emeritus and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law Emeritus*

Richard L. Barnes, *Professor of Law and Leonard B. Melvin, Jr. Distinguished Lecturer in Law*

Deborah H. Bell, *Professor of Law, Mississippi Defense Lawyers Association Distinguished Lecturer and Director of the Civil Legal Clinic*

Kristi Bowman, *Visiting Professor of Law*

John R. Bradley, *Professor of Law*

Phillip W. Broadhead, *Director, Clinical Appeals Program and Clinical Professor of Law*

Charles Brower, II, *Croft Associate Professor of International Law and Jessie D. Puckett, Jr. Lecturer in Law*

Mercer E. Bullard, *Assistant Professor of Law*

Larry Bush, *Professor Emeritus of Law*

William M. Champion, *Professor Emeritus and Mississippi Defense Lawyers Association Distinguished Lecturer Emeritus*

Thomas K. Clancy, *Director of the National Center for Justice and the Rule of Law and Visiting Professor of Law*

George C. Cochran, *Professor of Law*

Aaron S. Condon, *Professor Emeritus of Law*

John M. Czarnetzky, *Associate Professor of Law and Mitchell, McNutt, and Sams Lecturer*

Donna Davis, *Associate Professor of Law*
Jason Derrick, *Acting Assistant Professor of Legal Writing*
Kyle Duncan, *Assistant Professor of Law*
Thomas R. Ethridge, *Professor Emeritus of Law*
D. Michael Featherstone, *Professor Emeritus of Law*
Molly Fergusson, *Acting Assistant Professor of Legal Writing*
Joanne I. Gabrynowicz, *Director of the National Remote Sensing and Space Law Center and Research Professor of Law*
Kris L. Gilliland, *Director of Law Library and Associate Professor of Law*
Christopher Green, *Assistant Professor of Law*
Karen O. Green, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*
Matthew R. Hall, *Assistant Professor of Law*
Timothy L. Hall, *Associate Provost and Professor of Law*
Marc Harrold, *Counsel for National Programs and Visiting Professor of Law, National Center for Justice and the Rule of Law*
Michael H. Hoffheimer, *Professor of Law and Mississippi Defense Lawyers Association Distinguished Lecturer*
Robert C. Khayat, *Chancellor and Professor of Law*
Patricia Krueger, *Acting Assistant Professor of Legal Writing and Director of Academic Excellence Program*
Kate Margolis, *Visiting Professor of Law*
Don Mason, *Associate Director of the National Center for Justice and the Rule of Law and Lecturer*
Kali Murray, *Assistant Professor of Law*
Gary Myers, *Professor of Law*
Jack W. Nowlin, *Associate Professor of Law and Jessie D. Puckett, Jr., Lecturer*
E. Farish Percy, *Assistant Professor of Law*
Larry J. Pittman, *Professor of Law and Jessie D. Puckett, Jr. Lecturer*
Lisa S. Roy, *Assistant Professor of Law*
Ronald J. Rychlak, *Associate Dean for Academic Affairs, Professor of Law and Mississippi Defense Lawyers Association Lecturer*
Paul M. Secunda, *Assistant Professor of Law*
Jacqueline Serrao, *Associate Director of the National Remote Sensing and Space Law Center*
Hans P. Sinha, *Director of Prosecutorial Externship Program and Clinical Professor of Law*
Carolyn Ellis Staton, *Provost, Vice Chancellor for Academic Affairs and Professor of Law*
Robert A. Weems, *Professor of Law and Butler, Snow, O'Mara, Stevens and Cannada Lecturer in Law*
C. Jackson Williams, *Director of Legal Writing Program and Acting Assistant Professor of Legal Writing*

MISSISSIPPI LAW JOURNAL

PUBLISHED BY STUDENTS AT THE
UNIVERSITY OF MISSISSIPPI SCHOOL
OF LAW

VOLUME 76 WINTER 2007 NUMBER 3

COPYRIGHT © 2007, MISSISSIPPI LAW JOURNAL, INC.

Editor-in-Chief
JOSHUA S. KYLE

Executive Editor
TRESA BARKSDALE

Articles Editors
JARED W. EASTLACK
MICHAEL J. GORMAN
NANCY WILLIAMS

Notes & Comments Editor
DAVID A. O'NEAL

Managing Editor
RYAN PRATT

Business Manager
KATIE HILL

Mississippi Cases Editor
KATHRYN E. WETHERBEE

Developmental Editor
NICHOLAS B. HOLTZ

Symposium Editor
KATE MAULDIN

Membership Director
MARY CLIFT HITT

Office Manager
JAKE DICKERSON

ASSOCIATE EDITORS

Articles Editors
AMANDA BECKETT
JIM FARRELL
JOSEPH W. GILL
ELEANOR LAPORTE
KARA LINCOLN
KATHLEEN SHIELDS

Mississippi Cases Editors
EMILY FERRIS
CAMPBELL MCLAURIN
SLATES VEAZEY

Notes & Comments Editors
LOREN HENAGAN
MAGGIE MAYNORD

Administrative Assistant
PEGGY C. NAIL

Faculty Advisors
DEBORAH H. BELL
JOHN CZARNETZKY
ROBERT A. WEEMS

Staff

Elizabeth Archer
Casey Butts
Robert L. Bouis, III
Nathan Burrow
Michael E. Carr, Jr.
Andrew Coffman
Claire Cowart
Hunter Chandler
Jacob Delaplane
Kathryn E. Dennis
Jonathan Festa
Jennifer Forman
Taylor Heck
Tyler L. Harris
Alexandra Hutton
Molly Jeffcoat
Josh Johnson
Brent Klein
McCann Lefeve
William A. Lewis
Courtney Leyes
Eric McAdamis
Caroline McKibben
Taylor McNeel
Alysson Mills
Scott Murray
Ryan O'Beirne
Eric Patterson
Frank Pellegrino
Ronnie Wade Robertson
Lane Rice
Clare Smith Rush
A. Nicole Seale
Natalya T. Seay
Rex M. Shannon, III
Joseph Tullos
Amanda Wallis
Kim Watson
Lane Williamson
Andrew R. Wilson
Parker Y. Wiseman

Mississippi Law Journal

**Published by Students at the
University of Mississippi School
of Law**

VOLUME 76 WINTER 2007 NUMBER 3

Copyright © 2007, Mississippi Law Journal, Inc.

TABLE OF CONTENTS

SYMPOSIUM

PROSECUTION RESPONSES TO INTERNET VICTIMIZATION

**Sponsored by the
National Center for Justice and the Rule of Law**

FOREWORD
. . . . *Thomas K. Clancy* i

KEYNOTE ADDRESS: PROSECUTION RESPONSES TO INTERNET VICTIMIZATION
. . . . *The Honorable M. Jane Brady* 623

INTERNET AND COMPUTER RELATED CRIME: ECONOMIC AND OTHER HARMS TO ORGANIZATIONAL ENTITIES
. . . . *Edward M. Roche* 639

TECHNOLOGY, STALKING AND DOMESTIC VIOLENCE VICTIMS
. . . . *Cindy Southworth and Sarah Tucker* 667

CHILD PORNOGRAPHY AND FIRST AMENDMENT STANDARDS
. . . . *Kyle Duncan* 677

SHOULD ONLINE DEFAMATION BE CRIMINALIZED?
. . . . *Susan W. Brenner* 705

PANEL DISCUSSION I: THE DECISION TO PROSECUTE 789

PANEL DISCUSSION II: PREPARING THE CASE AFTER THE DECISION TO PROSECUTE HAS BEEN MADE 821

PROSECUTING THE INTERNET FRAUD CASE WITHOUT GOING BROKE
. . . . *Patrick E. Corbett* 841

PANEL DISCUSSION III: WORKING WITH CORPORATIONS ON CASE INVESTIGATIONS 875

SENTENCING POLICY AND PROCEDURE AS APPLIED TO CYBER CRIMES: A CALL FOR RECONSIDERATION AND DIALOGUE
. . . . *Donald R. Mason* 903

INTERNET CRIME VICTIMIZATION: SENTENCING
. . . . *John F. Curran* 909

THINKING THROUGH SENTENCING IN COMPUTER HACKING CASES: DID THE U.S. SENTENCING COMMISSION GET IT RIGHT?
. . . . *Richard W. Downing* 923

CREATIVE SANCTIONS FOR ONLINE INVESTMENT FRAUD
. . . . *Jayne W. Barnard* 949

FOREWORD

Prosecution Responses to Internet Victimization

Thomas K. Clancy[*]

The National Center for Justice and the Rule of Law,[1] a program of the University of Mississippi School of Law, focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. In furtherance of its mission, the Center has established the *Cyber Crime Initiative*. This initiative provides educational opportunities for judges, prosecutors, law enforcement, and law students to learn about computer-related crime and develops projects to facilitate the prosecution of persons engaged in sophisticated criminal activity. The projects become the focus of national conferences and produce innovative training materials and prototypical approaches to help states combat computer-related crime.

---

[*] Director, National Center for Justice and the Rule of Law, and Research Professor, University of Mississippi School of Law.

[1] The National Center for Justice and the Rule of Law is supported by a grant from the Bureau of Justice Assistance, Office of Justice Programs, of the U.S. Department of Justice. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in the articles stemming from the conference are those of the author and do not represent the official position of the United States Department of Justice. For more information about the Center, please visit www.ncjrl.org.

On April 4-6, 2006, the Center held a conference entitled *PROSECUTION RESPONSES TO INTERNET VICTIMIZATION*. The conference focused on identifying the dimensions of victimization, including of individuals and of entities but explicitly excluded discussion of international issues. It also was designed to focus on the responses of state and local prosecutors to victimization. It did not discuss what private parties, such as individuals or corporations, can do either to prevent the problem or what private remedies are available. The conference was sponsored by the Center, in cooperation with the National Association of Attorneys General, and was attended by representatives of Attorneys General offices from thirty-five states, American commonwealths, and territories. Also attending the conference were representatives from high-tech industry, the United States Department of Justice, and academics.

The Center believes that the conference, and the insightful articles published in this special edition of the *Mississippi Law Journal* that stemmed from the presentations at the event, further the Center's mission and, more importantly, make significant contributions to understanding the dimensions of Internet victimization and strategies to combat that growing problem. The Center, and I personally, wish to thank the participants for their contributions.

This edition of the law journal, as did the conference, begins with a keynote address by the Honorable Jane Brady, of the Superior Court of Delaware. Judge Brady is the former Attorney General for the State of Delaware and is nationally recognized as an advocate of victim's rights.

The remaining articles resulting from the conference, as was the conference, are organized around three themes. The first part examines the attributes and dimensions of Internet victimization: who are the victims? Clearly, a complete answer to that vast problem is not provided here. Instead, several aspects of the problem are emphasized.[2] Edward M. Roche, PhD., of the Information Policy Institute, takes on the task of measuring harm in his article, *Internet and Computer Related Crime: Economic and Other Harms to Organizational Entities*. Cindy Southworth, who is Director of Technology, the Safe and Strategic Technology Project, of the National Network to End Domestic Violence, and Sarah Tucker, examine *Technology, Stalking and Domestic Violence Victims*. Kyle Duncan, an Assistant Professor at the University of Mississippi School of Law, examines the Supreme Court's view of who is the victim in child pornography cases and adds perspective in *Child Pornography and First Amendment Standards*. Professor Susan Brenner, of the University of Dayton School of Law, who had been scheduled to speak at the conference but was unable to do so due to illness, proposes rethinking the current defamation standards in light of the changed circumstances of the Internet in her article, *Should Online Defamation be Criminalized?*

The second day of the conference focused on victimization issues that factor into criminal prosecution decision-making. Three panels and one special presentation examined aspects of that question.

First, there was a panel on *The Decision to Prosecute*. Leading that panel was moderator Marc Harrold, Counsel for National Programs at the National Center for Justice and the Rule of Law. Participating in that panel were Terry Berg, First Assistant United States Attorney, District of Michigan and, formerly, member of the cyber crime unit in the Attorney General's Office for the State of Michigan; Professor Patrick Corbett, an Associate Professor at Cooley Law School and another former member of the cyber crime unit in the Attorney General's Office for the State of Michigan; Todd Lawson, an Assistant Attorney General for State of Arizona; and Thomas Sadaka, who is a former Special Counsel in the Computer Crimes Prosecution section of the Office of State Wide Prosecutor for the State of Florida, and who is now in private practice. Each of these panelists has extensive cyber crime prosecution experience and lecture nationally on the subject. The panel discussion, reproduced here, addresses a variety of factors that prosecutors must consider when weighing the decision to prosecute a case involving the Internet.

---

[2] In addition, at the conference, Allison L. Turkel, of the American Prosecutor Research Institute, who is the Senior Attorney/Chief of Training, Child Abuse Programs, spoke about understanding adolescent and compliant victims.

The results of a second panel are also reproduced here. That panel discussed *Preparing the Case After the Decision to Prosecute Has Been Made.* Marc Harrold also moderated that panel, which consisted of John Grossman, who is Chief of the Corruption, Fraud and Computer Crime Division, and an Assistant Attorney General, for the Commonwealth of Massachusetts; Richard Hamp, an Assistant Attorney General for the State of Utah; and Jean Smith Vaughn, Chief of the Computer Crime Unit and a Special Attorney General for the State of Mississippi. The three panelists all have extensive experience litigating cyber crime cases and their comments provide valuable insights on the preparation phase of a criminal case.

Professor Corbett presented a special lecture and an article on *Prosecuting The Internet Fraud Case Without Going Broke,* to illustrate the point that Internet related-prosecutions are feasible and do not have to be fiscally prohibitive for state and local prosecutors to pursue.

The final panel provided a corporate perspective on cyber crime's impact and the commonality of interests that corporations and government have in assuring the safety of the Internet. That panel, entitled *Working with Corporations on Case Investigations,* was moderated by Hedda Litwin, who is the Cyber Crime Counsel for the National Association of Attorneys General. That distinguished panel included: Jack Christian, who is Trust and Safety Counsel, eBay, Inc., who discussed many of the ways that eBay cooperates with law enforcement; John Deerin, Vice President and Director of Security at the Bank of Tampa, who focused on banking practices; Michael Robinson, U.S. Anti-Piracy Director for the Motion Picture Corporation of America, who discussed how online piracy affects the movie industry; and Thomas Sadaka, who added the perspective of a former prosecutor who now works with corporations in the area.

The third day and the final part of this edition of the *Mississippi Law Journal* examine aspects of sentencing as it relates to Internet victimization. Don Mason, the Assistant Director of the National Center for Justice and the Rule of Law, served as coordinator for this part of the conference. His remarks, *Sentencing Policy and Procedure as Applied to Cyber Crimes: A Call for Reconsideration and Dialogue*, are expanded upon here. As Professor Mason notes, "very little attention has been given to post conviction matters such as sentencing, victim impact, or alternative resolution" in the cyber crime area. The presentations at the conference and the resulting articles are designed to begin to address those deficiencies. In *Internet Crime Victimization*, John F. Curran, Vice President and Deputy General Counsel of Stroz Friedberg, LLC, takes on that difficult issue. Richard Downing, of the U.S. Department of Justice, Criminal Division, Computer Crime & Intellectual Property Section, provides his perspective in *Thinking Through Sentencing in Computer Hacking Cases: Did the U.S. Sentencing Commission Get it Right?* Finally, Jayne W. Barnard, the Cutler Professor of Law at the College of William & Mary School of Law, discusses *Creative Sanctions for Online Investment Fraud.*

No one conference or one series of articles can address all of the vast challenges that the Internet has created. It is our hope that the reader will find these articles insightful and helpful in understanding and addressing those challenges.

KEYNOTE ADDRESS

PROSECUTION RESPONSES TO INTERNET VICTIMIZATION

The Honorable M. Jane Brady[*]

JUDGE BRADY: Well, thank you very much and welcome to everybody from all over the country. I wanted to say thanks to Tom Clancy and to Ole Miss for this invitation and for the existence of the National Center for Justice and the Rule of Law. It is just a tremendous program.

I first came down here at the invitation of then-Chair of the Criminal Law Committee for the National Association of Attorneys General, Patrick Lynch of Rhode Island, who had a conference here on Internet crimes. And, when I went home, it was kind of neat being able to tell people I had dinner with Tom Clancy. Everyone assumed that I knew the author of *The Hunt for Red October* and had the inside story on that. So you have a nationally recognized name, and, I believe, a nationally recognized program.

The outstanding aspect of this program is that it honors the prosecution function and puts it on an even balance, unlike many of the law schools around the country. It recognizes the valuable public service asset that prosecution is. In many law schools around the country their public service programs are to help the indigent or to help people with the civil litigation issues of victimization in domestic violence, but they fail to include, even if they have a prosecution externship program, they fail to include it in their public service array. I think it is really forward thinking to have recognized the value of the public service of prosecution.

---

[*] Superior Court Judge, State of Delaware; Former Attorney General, State of Delaware

As I said, I was here in May of 2005 and we went through an entire conference on Internet crime and I went up to Tom and said, "Do you realize that, in this entire program, I think we heard the word victim twice? There's a whole aspect to Internet crime that goes beyond the hardware and software and detection devices—the people who are at the other end of that Ethernet or phone line or wire." And, as a result, this conference was initiated.

I was very honored when they invited me to come back as the keynote speaker for this conference. Let me explain that the reason I served on the National District Attorneys' Association Board of Directors is because, in Delaware, the Attorney General is the DA. Rhode Island and Alaska are the other two states where that is true. And so, we have no elected prosecution officials on a countywide basis. I had the enviable opportunity to serve, not only as the attorney general, but also as the district attorney for my entire state and we prosecuted, literally, tens of thousands of crimes a year. And, I was a prosecutor in that office for twelve and a half years before my election.

So, I have personal experience with the victims of crime in handling my own cases as well as the perspective of policy, broad legal parameters, and the social issues as a result of my experience as attorney general.

About four months ago, as Tom said, I was appointed to the bench. My tasks and responsibilities have changed. But I don't think that, so long as I keep my remarks balanced and factual, that I will give reason to the concern that my superiors on the bench had regarding speaking about victimization at this conference.

So, now that I have given that disclaimer, let's get on to what I really want to talk about, which is how do we deal with the issue of victimization in these crimes? And, what are the special issues related to victims of Internet crime? I have put together an outline and some comments as to a number of issues, but let me say, first and foremost, that you are going to get a lot of statistics.

I've looked at the tremendous materials in the booklet that you received and have noted the tremendous qualifications of the speakers who are going to come after me. I want to try to give a broad overview of why this issue is important to victims and should be important to you, in terms of assisting victims, but I also put together this outline that takes us from the detection and the investigation to the prosecution and the resolution, because, of course, we all know that the prosecution is not the end of the case for victims. We also need to consider how to help resolve their victimization. And I am going to follow that outline generally, but I will also be extemporaneous on a few occasions based on some recent events and your comments.

I also wanted to comment on the array of services that Attorneys General's offices offer because Jonathan Raven, from the California Attorney General's office, and I worked on a survey last year of Attorneys General offices around the country, which showed that about seventy-three percent, if I recall the number, offer a victim service component. So if you, in your capacity, don't have regular contact with that component, then I encourage you to do so. Get to know where in your office that sits, who in your office provides the services, whether they are well utilized, whether they can be better utilized. Most instances of the crimes that you are going to address at this conference are going to fall to your offices, even in jurisdictions with active District Attorneys, more than most other types of crimes. That is because there is considerable expense, equipment and expertise that are required to investigate and detect these crimes. There have already been regional and federal initiatives on training, and there are going to be more, and the larger offices, with more training dollars are going to be looked to for assistance.

Today the real world is the cyber world. When you look at a survey that was done by PUE, the Internet project, they found that seventy-two percent of all adults use the Internet and eighty-four percent of people eighteen to twenty-four. Eighty-four percent! Eighty-three percent of people thirty to forty-nine, so, overwhelmingly, anyone under fifty is on the Internet and the statistics show that. Interestingly, seventy-nine percent, which is a higher percentage than most of the other breakdowns, of English-speaking Hispanics are using the Internet.

This was a national survey conducted between September of 2004 and May of 2005. Nearly ninety percent of those people who have a college degree and make more than forty thousand dollars use the Internet and the majority of them identify home Internet use at nearly the same rate as they identify office Internet use. Involvement with the Internet is not just associated with the workplace; it is also in the home. And, when asked, "Why do you use the Internet?," only about half of them said they use the Internet to do research for work; ninety-one percent of them use it for email. By the way, in my research for this conference, I also learned that the average American worker that has a computer at work gets about ninety emails a day. Talk about Internet victimization!

In addition, of course, many of them use the Internet for research related to their personal interests, directions, and other similar purposes. Interestingly, by the way, in the same survey, conducting banking or purchasing stocks, things like that—about twelve, thirteen percent. You hear a lot about adult content on the Internet and dating services on the Internet and the associated victimization issues that they hold. In the survey, only four percent admitted to viewing anything with adult content on the Internet and only nine percent admitted to looking for Mr. or Ms. Right on the Internet. That is a very small percentage, actually, compared to what the perception is about such use. But, as you can see, the reality is that today the real world is part of the cyber world. And it is going to impact people in very, very real ways.

Now, much media coverage, and therefore the prevailing perceptions, of Internet victimization is largely regarding child solicitation for sex, financial scams and frauds, pornography, or hacking. And, I will address those, but first, I want to talk about the broader picture.

Let's first address detection. The detection of Internet victimization can prove very challenging. If you were to Google "Internet victimization," which I did just to see what would come up; you would get one million, one hundred ten thousand hits in eleven hundredths of a second. So if you are a police officer trying to sort through what's going on on the Internet, you are going to be inundated and you're going to have to be very specific and try and detect the kinds of crimes that are occurring on the Internet through more discerning investigative tools.

There is clearly public awareness of the fact, as evidenced by all of these articles on Internet victimization, that it is occurring, but detection remains very elusive. Legal issues about where the victimization occurs when it is Internet crime. Practically, it occurs inside your bank account, inside your IT system, inside your living room, and, in many instances, in the context of serious and violent crimes, although they involve remote contact, it invades right into the victims' mind. It affects the victims' sense of well being, security, and safety.

The impact is particularly challenging for victims if, like in so many instances, they are participants in the crime because they either responded to an email, or invited contact, or somehow engaged with the perpetrator online. There are a lot of additional issues that these victims have to address, many of which we most often have seen in domestic violence or sexual abuse cases, but now can occur in many other types of cases. And, instead of personal confrontation, the way that these offenders get into your living room, or into your business, or into your bank account is not with a gun, it's remote. They don't put themselves at personal risk to commit the crime.

And so, the usual methods that law enforcement has used to detect crime—fingerprints, hair and fiber transfers or DNA—are really not available to help the police. And that kind of evidence is not only useful in determining the identity of the perpetrator, but can also provide other clues, such as the manner in which the crime occurred, and the location or locations where the crime occurred. Those questions are not so easily answered when the crime is committed through the Internet.

The fingerprint could be oceans away and the identity could be a pseudonym, the true identity of which could be very, very difficult to find. I mentioned earlier that one of the challenges is determining where the crime occurred. Now we all know there are the occasional issues of jurisdiction and territorial disputes. You know the usual territorial disputes—"It's mine. No, it's mine. No, it's mine." And everybody wants to prosecute the crime. Well, with Internet victimization, it could easily be, "It's yours. No, it's yours. No, it's yours." This occurs because the laws may be unclear or because the expertise and expense in both detecting and following through with the investigation and successful resolution of those criminal cases is so difficult.

There are challenges to educating and equipping law enforcement to be able to detect and investigate these crimes. Some efforts have been undertaken. There's a new training center in San Diego, which is a pilot for a number that are hoped to be located around the country. This kind of training for people who are assigned to detect, investigate, or prosecute Internet crime is critical. These professionals need to have an understanding of the hardware and software issues, to understand the mechanics of the technology.

Getting the cooperation of business is very important in the successful detection of Internet crimes because the Internet service providers are the people that are the key to finding out who lies behind—what face lies behind some of those crimes. I recall my frustration with the unsolicited spam emails, particularly the pornographic ones. I found out that every time you click on the link and go to the site, there's a penny or two pennies that is paid to the person or entity which sent it.

So I told my investigators, "Let's follow the money." Well, it was not as easy as I thought it was going to be. And getting cooperation of the Internet service providers is important. Virginia was able to do that with AOL a few years ago in an incredibly successful prosecution, one of the first in the country. Delaware has a great law on the books. We haven't really been able to use it very much because we don't have the information to be able to identify the perpetrators and bring them to justice.

Now let's take a look at detection from the victim's perspective. I saw in the materials that you are going to talk a little more in depth about this, but many Internet crimes are not reported, particularly financial crimes. As any of you who have worked with seniors who are scammed over the phone, who are scammed at their front door, or in an affinity fraud scheme know there is a great deal of embarrassment and a great deal of self criticism about their exercise of judgment. They are reluctant to report it; they are reluctant to acknowledge that they were a victim of a fraud.

There are reasons for that. If you are twenty-nine and make a stupid decision and are victimized, you and others conclude it is because you made a stupid decision. But, if you're seventy-nine and you make a stupid decision and are victimized, everyone thinks you are beginning to lose it. And so, there's an incentive for older people who don't want to lose their independence not to report these crimes. Similarly, with financial crimes over the Internet. In the same study to which I previously referred, about thirty percent of people over sixty-five are using the Internet on a regular basis. My dad is eighty-one, and he is a day trader. He's got eight monitors lined up on two shelves over his computer. And so, he's very active on the Internet. But others, like my mother, use the Internet mainly for email. But, even though there are only about thirty percent of those over sixty-five on the Internet, they still are targeted. Specific scams are intended to appeal to individuals who are retired, on fixed income, or a veteran. Many of the scams are intended to reach out to people who would be more likely to respond because of their life experiences, and their status or situation in life at sixty-five or older.

But, it's not just the financial crimes against individuals that go unreported. Law enforcement faces the same situation with financial crimes against businesses. You are going to hear some more about this, but it's true. Businesses and even the government are afraid to report a hacking because the fact that their system could be compromised because it could encourage someone else to do it. And, there are other scams against businesses. False invoices is a favorite one. A false invoice will be sent over the Internet, complete with authentic-looking letterhead or logo, for services that have been rendered. The bookkeeper pays the charge, and, in many instances, that is the end of it. If they are careful and not too greedy, these scam artists can get away with a lot of money. Even when detected and even if it involves a substantial amount of money, businesses are very reluctant to prosecute. They are willing to suffer their losses, and they don't want to be involved with the court system or with the police in the investigation or prosecution of the case.

They also, though, don't want anybody to learn, either from testimony in a trial or otherwise, how a person hacked into their system or where the gaps are in their security. There's a group called InfraGuard that has worked with businesses to try to prevent technology crimes, so that victimization doesn't occur.

InfraGuard is a federal program under the FBI that works with businesses to not only prevent, but also address hacking and other kinds of economic terrorism that might occur. I went online the other day and paid a bill in four seconds. It was great. We can do so much on the Internet, but we are so vulnerable with regard to access to all our personal information. And while we are not addressing international issues in this conference, you should know there are actually websites out there, most of them outside this country, that sell your personal information and your accounts online. Suppose they have access to an account in a credit union with forty thousand dollars in deposit. They will sell it on the Internet for five hundred dollars. And they actually post that product online. So, there's a lot to be said for assuring that your financial institution has the best security possible. The InfraGuard program's public-private partnership is working very, very hard to assure good integrity in the technology that supports the financial, and other, institutions in this country.

But, while uncertainty of one's own judgment may be an issue in Internet financial crimes, in the other kinds of crimes that we have talked about and you are going to see in your materials on Internet victimization—the child sexual abuse, the pornography, the solicitation for sex—there is a new element that those who assist victims must acknowledge. Many of them, fortunately, when they are reported, are detected in time to avoid significant harm. If the child reports something or the parents suspect something is wrong and the crime is detected in time, the police pretend to be the child and they intercept the offender before he has access to the child that he solicited online. The crime most feared has not occurred, but the imagination of what might have happened could exceed even the crime that might have occurred. And, for those instances of bullying and the other kinds of harassment and intimidation that occur on the Internet, there can be significant psychological reactions that present real challenges for you to deal with in serving those victims.

First, the young victims, let's talk about those because there are some findings I think are very concerning about those crimes. At least, according to a survey that was done by one child-oriented organization, about fifty percent of the kinds of threats or incidents that should have bothered children, the kids said didn't bother them. So I started thinking about that result and about what was going on with kid victimization and it occurred to me that maybe kids don't really see the cyber world as a real world. Maybe they see it as a fantasy world.

An incident in Delaware recently helped substantiate that thought. A local radio station disc jockey went onto a website similar to MySpace.com where kids from the local high school were posting pictures and descriptions of themselves. In one, a student had a gun, and he and a number of the other boys described themselves as "gangstas." Girls were describing themselves as "hos" and they were showing pictures of their buttocks and doing things that they did not normally do. They became very upset when the radio announcer read from the website, without, mercifully, using their actual names. They were incensed that he had invaded their privacy. It was a very enlightening moment for me, because they had no appreciation of the response they were inviting by what they were doing.

I saw how vigorously these kids reacted and were offended. They called into the radio show, they picketed, they were very offended that someone would take their personal information and put it out on the radio. They failed to appreciate that it was on the Internet for everyone to see. Many of them engaged in this banter that could get them in over their heads, not appreciating that it is real.

I am very concerned that they will not appreciate what can occur unless we educate and inform these young people. There are girls and boys, today, who are putting pictures of their buttocks, breasts, and genitals on the Internet. They fail to appreciate that first, it is publicly displayed; and second, that once one person downloads it, it is there, potentially, forever. It is there, potentially, forever. So it is important that we inform kids about the fact that these exchanges are not just between them and that is not just their space, that it is cyberspace. And that Myspace.com is in every space.

We have all heard the stories about the undercover police officer going online, posing as an eleven year old girl, or pretending they are fifteen and buying Viagra online. The truth is that the police can detect and investigate these crimes as remotely as the offenders. Instead of walking the beat, cyber detectives are letting their fingers do the walking. And they are getting pretty good at discerning how they should work to detect the kinds of predators that work online.

I meant to bring a statistic with me and forgot it. Maybe one of the other speakers will cite it. Several studies have found that approximately one in five kids reported having received a sexual solicitation online. The most remarkable thing, and the statistic I can't put my finger on, is that in the chat rooms, when the predator thought that they had a victim or a potential victim, the conversation turned to sex within thirty seconds or sixty seconds of the contact. The study found that after three or four IM exchanges or chat exchanges, they were already approaching sex. Know why? They don't want to waste their time. They don't want to waste their time. And so, for kids who are unprepared for any such event, a situation can get out of hand very quickly.

Now, suppose the police have done a great job of detecting and investigating a crime and they figured out who did what and they bring it to the prosecutor, or your office. You look at your laws and you think, "Okay, I'm supposed to prosecute this case. What law was broken?" Harassment, stalking, the way that we traditionally have defined those crimes, does not include anything except personal contact. Delaware and most states did add contact by phone and mail. But, over the past several years, states have had to again change their statutes to include crimes committed by computer and Internet because they were not included in the previous statutes. And so, did it fit? Did it not fit? We argued the phone line back in the old time days of dial-up access to the Internet, which only thirty to forty percent now still use.

We argued that access was by the phone line and that the instrument at the end of the line didn't matter. We never went to trial or had the court resolve that issue, but that was one of the ways we tried to approach it. How many of your states, now, have added a specific Internet or computer crimes that would apply to harassment and stalking and everything? I see a little over fifty percent, have responded affirmatively.

When you go back to your offices, look at your laws. You know the attorney general is a statewide official and can be very effective in getting the state statutes changed to adapt to the changing technology by which criminals are taking advantage of the legislature's constituents. So go back and look at your laws. And if your laws are not adequate to the crimes that you are seeing and you are going to learn a lot more about in detail through this conference, look at your laws and make proposals to fix them. Look at what the other states do and figure out what will work best in your state. That is one of the first inquiries that you need to make.

So, first line of analysis—"What does the law allow?" If you get an Internet case, what does the law provide? The second is "Where did the crime occur?" Many times, the issue of the location of the crime will be resolved in the prefatory sections of your criminal code in your state. The code may say that if any element of the crime occurs in your jurisdiction, you can prosecute. Others say, if the overt act by the perpetrator occurs in your jurisdiction, you may act. And there are some which provide that if the harm to the victim occurs in your jurisdiction, you have authority.

So, figuring out whether you have jurisdiction to prosecute this crime is another issue. To the victim, that means a great deal. If you don't have authority to prosecute the crime where the victim is, it is another impediment to getting their cooperation and successfully prosecuting a person who's committing a crime because that victim will be required to go to another jurisdiction.

And, if you are talking about young victims whose parents are concerned about them participating in a trial where the offender will be able to see the victim—remember, the offender likely never knew what the victim looked like before. It is going to be a significant impediment to keeping their cooperation if they have to travel to another jurisdiction and may never develop a rapport with the prosecutor or victim services worker.

So, consider what is, for the victim, the best place to be for prosecution. Look at your laws and figure out where you can prosecute the crime. And, while not all your victims are necessarily sympathetic, they all are vulnerable. So, how do you provide victim services to these victims?

I am not going to talk about how you generally provide victim services to victims of certain kinds of sexual crimes or domestic violence crimes or stalking crimes because you've done that. But I will talk about what happens with the victims in certain situations—I call them the balks. Everybody knows baseball? Okay. The balk is where you start the pitch and you don't let go of the ball. Okay? And it's a penalty.

That can happen to victims in these Internet victimization cases, particularly the solicitation cases. In those which are detected or reported, the greatest harm that could have occurred does not. The fear of what might have happened is, however, often more difficult to face than the certainties which other victims to whom a harm has occurred learn to address. The latter have some tangible event, some consequence, which they can address emotionally, try to understand, and with which they can begin to cope. Often, with Internet victimization, the actual event is a balk, and the fear of what might have happened can be very, very devastating to family members and to the victims themselves. It can become their very own version of terrorism that prevents them from appropriately interacting and engaging socially and at work.

And so, there may be unique issues in serving these young victims and their families who sit and worry about everything that might happen now because they can't associate one bad act with one bad person. Just as the Internet is ethereal, there is an ethereal threat that is ever present to them.

I mentioned, also, that many of these victims lose confidence in their own judgment. This applies not just to financial fraud victims, seniors and others who are challenged.

Finally, for victims, it is not just the success of law enforcement or the prosecutor. For victims, it is "How do I go forward—emotionally and psychologically?" There are some things that are being done for victims of Internet victimization. The National Organization of Victim Assistance is a group with which I served, which has often dealt with crisis response. Their models of crisis response for these balk cases I was talking about, many of the responses for crisis—models for crisis response—can work for this kind of Internet victimization, where the fear and the anxiety and the emotional response is one that is of a lingering and continuing nature.

And, finally, how do you help the families of these kids with resolution? Just as in some rape cases, in which the family, who has been a protector, feels that they have failed, the same can be said in these Internet crimes. The guilt may be even more significant, however, because often in these cases the parents provided the computer or didn't monitor the child's use of the computer. They may have allowed the child to have a computer in the child's bedroom. In the realm of providing victim services, you need to consider those secondary, as we call them in Delaware, secondary victims, that is, those victims who are related to and affected by the victimization of the direct victim of the crime.

I've looked at the materials for this conference; they look tremendous, as I said. You've got some excellent speakers. This conference is going to provide the very best overview that I have ever seen on this issue, and good information on all aspects of Internet victimization. I hope that my overview has covered both the importance of being aware of and educated about Internet victimization and the role that you can play in the attorney general's office by reviewing your laws, educating your law enforcement, looking for where the financial resources are or the expertise is to draw upon to assist local jurisdictions in the prosecution of Internet crimes, and to provide adequate victim services for those victims of Internet victimization because, as I said, there are unique issues that they face, unique challenges that they pose for you.

And since the majority of AGs offices do provide victim services, this awareness needs to be a component of how you provide those services. If, today, seventy-three percent of all adults use the Internet and eighty-five percent of those eighteen to twenty-four are using the Internet, I think it is a good bet that, of those aged seven to eighteen, probably ninety-five percent are using the Internet. And soon, it is going to be universal, much like the telephone.

So there are some new and recent developments in the evaluation of the extent to which the Internet and crimes over the Internet are occurring and identity theft is occurring, much of which occurs over the Internet. I found a very interesting article about this man in Russia who is selling accounts online. He actually is advertising the accounts online. So, the more remote and the more junctures through which the email is routed, the more difficult it is to find out who's actually committing the crime.

And, of course, unfortunately, the further you get from home, the more difficult for you to prosecute it no matter what the harm to the victim. And the more international you get, unless it's a big case, you don't get the federal government's interest because they can't, and don't, prosecute every little crime.

So, good luck, enjoy the conference. I have to tell you, I spent eleven years as Attorney General of Delaware and I always wondered why anyone would want any other job. Everybody who has held or holds the position says it's the best job in the world. I, however, had always wanted to be a judge since before I became a lawyer, so I don't regret the decision.

But you have a tremendous opportunity to make a difference in your state, in the law, in the policy and the priorities of the agencies you represent, to impact the direction of the law enforcement community and the legislature in your states. And so, I encourage you to fully utilize the resources you have at your disposal and address the needs of the law—reforms in the law and in your offices to respond to crimes against your citizens via the Internet. Thank you very much for having me.

INTERNET AND COMPUTER RELATED CRIME: ECONOMIC AND OTHER HARMS TO ORGANIZATIONAL ENTITIES

Edward M. Roche[*]

There are different and conflicting reports estimating the value of Internet fraud [and related computer crime]. But serious issues abound regarding calculation of values. Here, cost estimations are broken down into three categories: (1) tangible, (2) intangible, and (3) operational. For each of these categories, we sub-divide into different classes of harmful effects, and then suggest several ways of making estimates. These include such approaches as (a) adjustment of under-reporting data, (b) use of insurance values to estimate reputation loss, (c) time & effort estimations for individuals [and many others]. We suggest how these estimations might be used in victim compensation, defined as either (a) government victims, (b) institutional victims [including business enterprises], and (c) individual victims. A major theme that emerges from this analysis is that (1) some of the considerably larger damages [costs] are more difficult to estimate, since they are speculative in nature, and (2) damages [costs] that occur either (a) internally [e.g., for the individual, inside the enterprise], or (b) more distant in time, from a practical point of view, generally in the absence of advance planning are extraordinarily difficult to calculate.

---

[*] Information Policy Institute, Chapel Hill, North Carolina, Director of Scientific Intelligence, See http://www.infopolicy.org. Home address: 135 East 54th Street, Suite 4-B, New York, New York 10022-4509 Tel: 646-416-6592. We would like to thank Mark Halligan, Chairman of the ABA Committee on Trade Secrets for providing information regarding trade secret protection and calculation of damages.

I. THE BUTTERFLY EFFECT

It simply is not possible to know the true cost of internet fraud [and related computer crime]. But it *may* be possible to *estimate* its value.[1]

In an ideal scenario aimed at making this estimation, we first define the scale and scope of the types of crimes being discussed. Then, for each *type* of computer crime, we discuss the adequacy of known data, the sources of error in the reporting, the reasons for those errors, and what can be done to correct the estimates. We then make estimates for each type, and add them together.

Although an overall sector-based approach to the problem might prove to be overly general, it represents a way that promises to yield a useful approximation of costs and value lost that is more accurate than the general overall summary figures reported in the press. It is a *taking apart* of those numbers.

Before going further, however, lets explore data from a series of interviews. Four examples are presented below. They will clarify how the costs involved range in nature from highly specific to highly *speculative*.

A. *Example One: Reputational Loss*

Lets start with an example of a U.K. bank that suffered an Internet fraud. It is a true case, but the name of the bank has been changed.

---

[1] The Butterfly Effect is a phrase that encapsulates the more technical notion of sensitive dependence on initial conditions in chaos theory. Small variations of the initial condition of a dynamical system may produce large variations in the long-term behavior of the system. This is sometimes presented as esoteric behavior, but can be exhibited by very simple systems: for example, a ball placed at the crest of a hill might roll into any of several valleys depending on slight differences in initial position. Wikipedia.com, Butterfly Effect, http://en.wikipedia.org/wiki/Butterfly_effect (last visited Oct. 31, 2006).

> *A major European bank suffered a compromise of its computer system when hackers managed to break in and deface one of the internal web sites. There was no direct economic loss to the bank. However, in line with regulatory and insurance requirements, the bank reported the incident. When word got out to "the street," e.g., to the financial markets, there arose a perception that the bank was unable to secure its information systems, and thus might pose a risk to investors. Consequently, the share price of the bank started to fall.*
>
> *Unfortunately, at this time, the bank was the subject of a hostile takeover bid from a rival bank. The predator was able to take advantage of this drop in share price and make a successful move in the market, thus acquiring the bank. Even though no money was lost due to the computer hack, the bank was sold off and lost its autonomy in the marketplace. The bulk of its top management was made redundant.*

The question that begs asking is this: If no money was taken from the bank, then how can there be a claim for financial loss? The hackers never were caught, so the issue did not arise. But there is the issue of possible insurance coverage.

To make matters even worse, subsequent auditing revealed that *the entire incident might not have happened as first reported.* Unfortunately, this "subsequent auditing" was done *after* the takeover was completed!

Clearly there was "loss," but it was a *secondary effect* of the reputational loss which itself was caused by the hint [later determined to be false] of a security weakness in the bank's system.

This example points to several issues including:

1. If there was no financial loss, e.g., no money stolen, then can the reputational effect be consid-

ered?[2]

2. If it *is* considered, then what is the basis of the loss calculation? For example, should it be the lessening of the value of the company in the stock market [or effects even beyond that]?
3. If the bank eventually was taken over, then were there additional damages that might be considered?
4. Are damages to the shareholders or to the bank itself, or to yet others?
5. Finally, if it could reasonably be expected that leakage of the facts to the financial markets might harm the share value of the company [in such a catastrophic way], then is it a responsible action to report, or is it more prudent to hold back the information?

B. Example Two: Failure to Report

The Chief Information Officer[3] of a large and well-established Swiss bank discussed his focus on computer security and the requests by some governments concerned about illegal money-laundering that their investigative services be given access to those encryption codes used for money transfers:

> *If our customers* EVER *learned we were cooperating with governments in this manner, we would lose* ALL *credibility in the marketplace. Customers come to our bank with a firm belief in the absolute security and confidentiality of their transactions. If anything at all changed this perception, it would be a disaster for us, and it would take an indefinite amount of time to recover.*

---

[2] Calkins lists reputation effect as one of the elements of an economic analysis of hacking. *See* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171 (2000).

[3] The Chief Information Officer (CIO) in most companies is responsible for the acquisition, management, and operations of all data processing and telecommunications throughout the enterprise. For [large] multinational corporations, the CIO might have several hundred persons reporting to them, and an annual budget of several dozen million dollars.

Even in these "private" and "off the record" discussions, the interviewee *never* made an admission of a security problem. But when asked about the situation *in the industry*, the CIO emphasized that it is *never* in the interest of a financial institution to report security problems. He believes the best way to cope with this situation is through "internal" processes.[4]

This example raises several questions including:

1. If the majority of organizations resist reporting Internet fraud [and related computer crime], then what is the meaning of reported crime statistics? For example, should any number reported be assumed to represent only a fraction of the actual problem? [Most would say "yes."]
2. Is it possible that the long-term damage from a relatively minor information security compromise might be far greater than the immediate harm that is inflicted? If so, then what can we conclude from a comprehensive report on the levels of immediate harm reported? Are we [again] only making an examination of a *fraction* of the actual amount?
3. What is the best strategy: to never report, or to invest much more in security in hopes that pre-

---

[4] Bazelon, Choi, and Conaty categorize failure to report as a variation of abuse of personal information. *See* Dana L. Bazelon, Yun Jung Choi, & Jason F. Conaty, *Computer Crimes*, 43 AM. CRIM. L. REV. 259, 290 n.238 (2006). De Villiers states that, "Firms seem particularly reluctant to report and prosecute cybercrimes that originate from overseas." See Meiring de Villiers, *Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare*, 4 NW. J. TECH. & INTELL. PROP. 13, 120 (2005). *United States v. Bajakajian*, 524 U.S. 321 (1998), is an example of failure to report illegal money transfers in banking is discussed by Starkey and Park in their review of the Bank Fraud Statute, the Financial Institutions Reform, recovery, and Enforcement Act of 1989 and the Bank Secrecy Act. *See* Jeffrey N. Starkey, Jason Park, & Matthew B. Novak, *Financial Institutions Fraud*, 42 AM. CRIM. L. REV. 497, 497 (2005). Finally, the distortion of computer crime statistics caused by underreporting is discussed by Bakewell, Koldaro and Tjia. *See* Eric J. Bakewell, Michelle Koldaro & Jennifer M. Tjia, *Computer Crimes*, 38 AM. CRIM. L. REV. 481, 483 (2001).

vention can work and avoid any embarrassment.

C. Example Three: Asymmetric Defense Costs

The manager of an important IT installation[5] was discussing the rapid increase in costs associated with defending against Internet fraud. He pointed out first the problem that *it is impossible to have complete security,* no matter what precautions are taken.

> *No matter how much we spend, we can never have complete security. All spending can do is LOWER THE PROBABILITY of a successful computer attack, but it can NEVER stop completely the problem. Eventually, any organization will reach diminishing returns on their security investments. We end up spending too much and getting in return virtually no increase in security.*

Second, he lamented the dilemma of so-called "asymmetric defense" issue:

> *Our problem is that it costs so little to launch an attack, and so much to defend against it. It is much like the failed attempts at strategic missile defense—a losing proposition. We can NEVER obtain complete security, even if we had unlimited resources, which we don't. THE ONLY QUESTION IS HOW MUCH INTERNET FRAUD CAN WE TOLERATE. THIS IS FOR MOST A VERY DIFFICULT QUESTION TO ANSWER, PARTICULARLY IN THE BOARDROOM.*

This example raises several questions including:[6]

1. Is it possible for an organization to define the level of Internet fraud [and the damage] it is willing to tolerate?
2. Who is empowered to make the decision regarding

---

[5] IT—"Information Technology"—a term used to represent all of the computing and telecommunications resources within an organization.

[6] For the formal theory of asymmetry, see Ivan Arreguin-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict*, 26 INT'L SECURITY 93, 93-128 (2001).

the level of security required, and the level of vulnerability allowed?

3. Should the cost of Internet fraud include the costs of defensive measures, even if no fraud takes place because the defenses appear to be effective?
4. And if defensive measures are included in the cost estimations, then how far does the analysis reach? For example, within the IT function alone? Throughout the enterprise? Hardware and software costs? Training and awareness costs? *All* security measures?

D. Example Four: Compromise of Individual's Information

In a large North East US based insurance company, several of the top executives started to get strange credit reports and bank notices. Evidently many had taken out mortgages, topped out their credit cards, and purchased many fancy consumer goods they had no recollection of ever needing.

Later investigation revealed that a trusted employee was the source of the information used to compromise the identity of *hundreds* of employees. As a database administrator [who had access to *all* personal information on the company employees], the employee sat in a cybernetic "cats bird nest." The information had been "brokered" to organized crime, then used in a variety of scams. The organizational leadership was shocked.

> *"How could one of our most trusted employees do this? and Why?"*

Any security consultant easily could have given them the answer. All of the "usual" reasons applied:

1. Gambling debts that must be paid off to the mob.
2. Resentment at not getting a promotion.
3. Anger at the company for not paying enough money "while top executives get rich."
4. Psychopathic behavior.

In this case, the "resentment" answer proved to be the best fit. For the company, firing the director of security was only the first step in a very long chain of events—investigative costs, litigation, administrative costs to improve security, re-screening of "trusted" employees, calling in a security consulting firm to "fix" the problem, conducting numerous "audits" to see if other problems could be detected, paying money to "public relations" consultants to make sure the reputational effects were minimized, e.g., "this was a freak accident, an aberration in behavior of a *single* employee, and not representative of our overall security"—all of which added up to a large number that never was completely calculated, and *certainly* never made public.

What was the "cost" of the attack: zero.

What was the "effect" of the attack: millions.

This example also raises questions regarding the cost of this Internet fraud crime. These include:

1. What is the total financial cost of this crime; what should be included and excluded?
2. How many crimes were there in all? [e.g., what is reported in the crime statistics?]
    (a) Initial theft of corporate information?
    (b) Conversion of the stolen information?
    (c) Use [by others] of the information for fraudulent purposes?
    (d) Individual crimes committed "downstream" from the original theft?
3. Should *all* of the investigative costs get included?
4. Should all legal and administrative costs be included?
5. In general, how wide should the circle of *secondary effects* be traced in order to evaluate the cost of this Internet fraud case?
6, When the database administrator is prosecuted, then how wide is drawn the circle of responsibility?

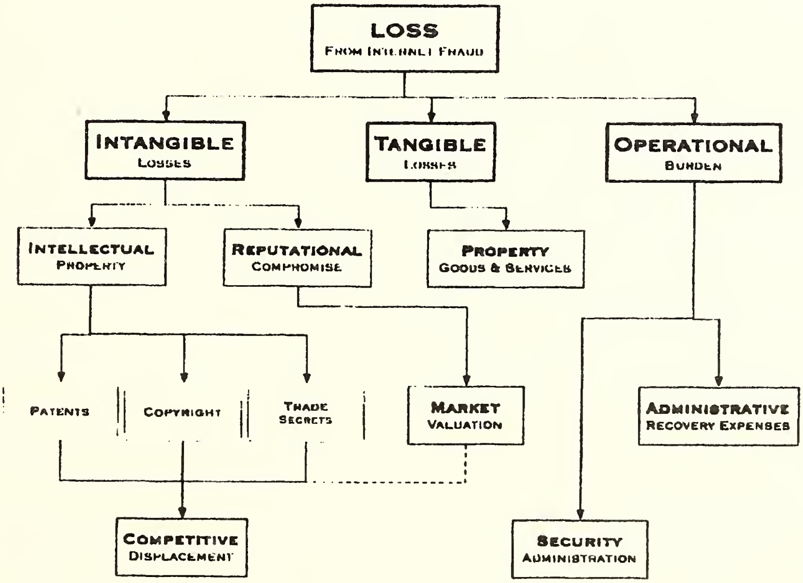
II. CLASSES OF LOSS

These examples and many others suggest several ways to characterize the losses from Internet fraud and abuse. In particular, they might suggest at least three major categories of loss. (*See* Figure 1 below.) These are:

TANGIBLE LOSSES. When Internet fraud is used to steal property, particularly to take delivery of illicitly gained goods, there is a tangible and identifiable type of loss. Although more abstract, the theft of services may fit in this category [and is easy to measure].

INTANGIBLE LOSSES. Internet fraud can cause serious damage *without* the theft of any property. In some sectors, such as banking, the reputational effects might be the largest to contend with. What is the complete range of intangible loss?

Figure 1: Categories of Losses from Internet Fraud


LOSS
From Internet Fraud
INTANGIBLE
Losses
TANGIBLE
Losses
OPERATIONAL
Burden
INTELLECTUAL
Property
REPUTATIONAL
Compromise
PROPERTY
Goods & Services
PATENTS
COPYRIGHT
TRADE SECRETS
MARKET
Valuation
ADMINISTRATIVE
Recovery Expenses
COMPETITIVE
Displacement
SECURITY
Administration

OPERATIONAL LOSSES. Any discovered loss[7] of necessity requires the expenditure of at least a minimum amount of resources in order to get back to normal. In addition, there is a significant amount of cost for general administration of security, including during the "clean up" phase after discovery of a compromise. What might be the details of this and what value does it comprise?

A. Tangible Losses

Internet fraud in many cases is aimed at the illicit taking of goods or services. Note that this objective is very different from computer crimes that *deny* services to others. The most popular of this class of loss is the stealing of money, every hacker's dream. According to a banking source:

> *One of the first great computer crimes involved a programmer who re-wrote the interest calculation in a bank's savings accounts to take the $ 1/1000-ths of a percent remaining from each interest calculation and have it transferred to a secret personal account. For a while they made lots of money, but it was difficult to say if they stole money, or simply created money from adding up multiple small transactions.*[8]

This type of crime still is with us today, with a similar theft taking place recently against a New York bank orchestrated by a gang of Russian hackers.[9] In another case, a programmer changed the shipping information for delivery of telecommunications equipment to a "dummy" warehouse. Millions of dollars of equipment was delivered [and subsequently diverted] before discovery of the crime.

We can say that depending on the type of fraud, real tangible losses may account for a considerable amount of loss.

---

[7] Note that it is estimated than less than 10% of Internet frauds are *detected*.

[8] Unfortunately, this rather fine legal distinction did not sit too well with the police and prosecutors who handled the case.

[9] It always is quite interesting to read the published accounts of computer fraud, with particular attention paid to any public statements made by the victim financial institution.

In addition, depending on how it is defined, the theft of services can as well be significant, although with increasing levels of computer security in society, this option each day is lessening as a possibility.

For the most part however, the *valuation* of the losses can be estimated by simply taking into consideration either the book value of the items, or the service cost as a function of the amount of time used [or another relevant metric].

B. Intangible Losses

Perhaps it is fitting that for hostile activity as *abstract* in its nature as is Internet fraud [an almost completely "information crime"], the largest losses might be "intangible," also of an "informational" nature. We can identify as among the most important two categories of intangible losses: (a) Reputational Losses; and, (b) Intellectual Property Losses.[10]

REPUTATION. In the second example—Failure to Report—we can see how the release of information regarding a relatively minor security incident can have disproportionate effects on an institution. There can be both long-term and medium-term effects. Examples would include:

1. Drop in the market capitalization of the firm as word "gets out" that has some type of security problem. Investors are unlikely to put their money back in until they are reassured, but for many, given the vast amount of investing possibilities, the problem even if fixed might deter re-investment.
2. Long-term "tarnished" effect on the firm where a reputation earned tends to "stick" in the minds of investors and customers, thus leading to *permanent* damages [in

---

[10] *See* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 362 (2005) ("The injury problem in cyberspace is based on intangible losses, unlike the disfigurement or pain and suffering experienced by the victims of physical injury. Nevertheless, these economic or information-based injuries are legally protectable interests."). For examples of specific loss calculations, see Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 932 (2003).

business (or other activities)].

Intellectual Property. Divided into three categories—(1) patents, (2) copyright, and (3) trade secrets—losses of intellectual property can have long-term and *devastating* effects on an enterprise. Generally there is a good understanding [and substantial historical record] for estimating the cost of patent and copyright violations.[11] Regarding patents, for example, one executive interviewed said:

> *We found that a Japanese company had copied completely our patented design, but they were so large, and we were so small, the prospects of litigation seemed daunting. Their production quickly out-paced ours, and then they started to modify and re-patent our ideas. When we went to the U.S. government for help, they turned a deaf ear. In balancing overall U.S. interests against our company's interests, guess who came out on top? At the time, the relationship with Japan was too sensitive to "rock the boat" with a case like ours. Eventually, we lost everything.*

However, in the case of trade secrets, a more complicated picture emerges. These "secrets" include [but are not limited to] the following types of information [and data]:

1. Customer lists;
2. Sales forecasts;
3. Workflow documentation;
4. Employee lists [and other details on employees (such as executive compensation)]; and,
5. Special knowledge for either manufacturing or other work processes.

Trade secrets consist of a very large range of types of data and information, and there is a corresponding great variety in the *motives* and *uses* for stealing them.[12]

---

[11] No need to discuss herein.

[12] Types of persons interested in trade secrets include: competitors who want

Unfortunately, valuation of trade secrets is problematical. Two examples will illustrate the reasons:

TIME VALUE. Over time, information that is a trade secret might become more valuable [or decline in value]. The result is that any *declared* value of the trade secret will diverge from the recorded [or declared] value.

EXTERNALITIES. Your trade secrets may change in value [may become worthless] depending on events you do not control, such as activities of competitors. What is valuable one day may be worthless the next. [NB: Related to "time value."]

SLOPPY ACCOUNTING. It is a fact that most corporations have not valued their trade secrets. If this is the case, it is difficult under examination to sustain the idea they are trade secrets at all, since *by definition* in order to be a trade secret, it must have value *that can be documented.*

In any case, it is the loss of trade secrets, whether valued or not, that potentially leads to the most chilling long-term consequences for the victim.

C. Operational Losses

The two major types of operational losses that are incurred as a result of Internet fraud [and related computer crimes] involve the activities that are compelled [to take place] as a consequence of the incident and the changes in operations that must be put into place in order to insure against any repeat of the event.

We have classified these as: (a) administrative recovery expenses, and (b) security administration [expenses].

ADMINISTRATIVE RECOVERY. As a consequence of any event, there is an immediate *forced* requirement that the organization take all necessary measures to bring the situation back to nor-

---

lists of customers, "discount" price lists, or documentation on workflow [and how your company gets its efficiency], foreign governments [or their front companies] who may have stolen patented information but need additional trade secret information to understand how to make the best use of what was stolen, or consulting firms who are doing "market research" or "competitive intelligence" research work [usually for your competitors].

mal. This would include activities such as:

1. Impounding of all internal records associated with the event.
2. Collection of statements from persons who have knowledge of the event.
3. Electronic data discovery and computer forensics.
4. *Analysis* of the electronic discovery.[13]
5. Legal expenses such as (a) preparation of complaints, (b) all of the 'downstream' activity associated with litigation.
6. Filing [and sustaining] insurance claims associated with the event.
7. Mobilizing [if needed] the public relations capabilities of the firm, including potentially the "crisis management center" to deal with the public [including financial analysts].
8. As needed, coordination with law enforcement [or other government authorities].

For these types of expenses, it would be customary to have easily a clear accounting of any *external* resources [advisors, experts] used, but for *internal* resources of the firm, it is critical repeat critical that a pre-arranged system be in place to account for the organization's personnel involved and their time commitment.[14]

SECURITY ADMINISTRATION. All organizations [even many individuals] have security expenses of one type or another. Should security fail, it signals that something has grossly failed, and consequently there is a need for a mandatory investigation, and revision of the procedures [or technologies] involved. In the case of Internet fraud [and related computer crimes], this involves several "sub-systems" of the security apparatus including:

---

[13] This can be extraordinarily expensive, and usually is done by outside [highly paid] experts.

[14] If this is not accounted for *immediately upon initiation of the recovery operation* then it is likely the real cost will *never* be credibly sustainable, e.g., there will be a complete absence of records to substantiate the claim.

> 1. ADMINISTRATIVE PROCEDURES. The organization must assess whether or not any administrative procedures failed. Examples would include: (a) accidental disclosure of confidential information, (b) vulnerability to a "social engineering" attack,[15] (c) failure in screening out criminal personnel, or to watch for signs of a compromised employee, (d) failure to train adequately personnel to protect information or systems, (e) human error in administering what is otherwise a relatively secure system.
> 2. INFORMATION SYSTEMS. Computer networks are protected by [among many other technologies] so-called "firewalls" that read through incoming data traffic to screen out malware or other types of threats. It is an unfortunate fact of life that firewalls [and other administrative software] can detect *only known threats*. Consequently, if a "hack"[16] is used for the first time, then *no installation* can have protections against it, and the threat will not be recognized.
>
> Firewalls receive in the press much recognition, but the largest expenditures in IT security include (a) password and access administration, including "help desk" services, (b) software and hardware systems that monitor and control network and system security, (c) the cost of designing, building and maintaining systems with excessive security [because the "hackers" leave one no alternative but to expend these costs.] NB: in many cases, item (c)

---

[15] SOCIAL ENGINEERING is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible. Wikipedia.com, Social Engineering, http://en.wikipedia.org/Social_ engineering_%28security%29 (last visited Oct. 28, 2006).

[16] Literally, a way of cutting through or "hacking through" computer security.

is the greatest because it involves re-design of entire systems.

When an incident occurs involving information systems, it usually calls for costly replacement or upgrading of equipment and systems. For most companies, this type of expenditure is a "must do" spend, and in many sectors [e.g., financial services] it is a *required* project [in order to maintain compliance with Federal regulations].

After an incident occurs, the organization must engage in a "mopping up" operation in which the information system—in a large enterprise comprised of *thousands* of computing devices is "sanitized" of any offending malware [or otherwise made invulnerable to a repeat of the same attack]. When a large-scale event takes place, these costs can be substantial:

> *When we were hit with the slammer virus, we lost on a worldwide basis all of our NT servers for email, applications, and database functionality. The entire company was unable to complete any office work for more than a week. Since the virus went into the directory services of the [operating system] software, we had to rebuild by hand EACH SERVER and we have hundreds of them. It took us a few days just to identify the problem and comprehend how it worked. Before doing anything to our infrastructure, we first had to develop a "patch," then test it thoroughly before using it. Finally, moving across our corporate network on a segment by segment basis, we got things up and running, but not before many trials and errors. I can't imagine how to calculate all of the total resources wasted in this event, but it was enormous.*

Consequently, we can see that the interviewee described *two* types of costs: (a) the nightmare of rebuilding an extensive infrastructure, and (b) the *loss of business productivity* that was generated as a result. Unfortunately,

> it is difficult to estimate the effects of temporary cut-offs of white-collar work, just as it is inherently difficult accurately to measure white-collar productivity.

PERSONNEL. It is said that more than 80% of Internet fraud [and related computer crime] is accounted for by either (a) "inside job" activities of your employees, or (b) mistakes. Other common problems are generated by (c) poor [or zero] training, or (d) compromised employees. Contrary to popular perception, resisting penetration by strangers *from the outside* represents only a small part of the total challenge.

Consequently, an organization usually must endure the following expenditures as a consequence of an event:

1. Termination and re-hiring of personnel.
2. Associated [usually litigation] costs with termination.
3. Associated [usually head-hunters or executive placement] costs with new hiring.
4. Probable salary differential [higher] for replacement personnel.
5. Re-training costs of new personnel.

III. USE IN VICTIM COMPENSATION

Victims of Internet fraud can be (a) governments, (b) institutions [including businesses], or (c) individuals. Consequently, the estimation of the cost of Internet fraud [and related computer crime] vary, and are based on different scales.

Regarding compensation for Internet fraud, we can make the following observations:

OBSERVATION 1. Due to the essential *asymmetrical* nature of Internet fraud, the perpetrator rarely has enough "deep pockets" if any at all against which and from which any significant compensation might be obtained.

> *Two years ago, a high school student in Malaysia released a computer virus. We picked it up in our subsidiaries in Asia, but were unable to stop it in Europe before it infected our North American operations. In*

> *addition to our problems, that single incident cost U.S. corporations several billion dollars damage. Although he said he was "sorry," from a practical point of view, there was no possibility of getting any type of meaningful compensation for the damages done.*

This is a universal problem when seeking compensation for Internet based fraud, and there are at least two equally frustrating variations:

1. The perpetrator has no "deep pockets" from which recovery might be taken; or
2. It is impossible even to *identify* the perpetrator.

Another variation is that even if the above two factors do not interfere, international jurisdictional problems [e.g., extradition], make it impossible to take any meaningful action.

OBSERVATION 2. Each Internet fraud generates a series of cascading effects—primary, secondary, tertiary, etc.—and like any tort there is a point in the chain of causation where the effect becomes so remote that sure causation is arguable. The practical result of this is that ultimately, the settlement of any compensation or restitution issue is unlikely to be strictly related to the actual harm caused. Particularly when considering the *intangible* aspects of the problem, one would suspect that more likely than not calculated damages will be substantially less than actual.

This leads to several tentative conclusions regarding the calculation of the costs of Internet fraud [and related computer crimes] for the different parties that are victims, e.g., governments, institutions and individuals.

A. Government as Victim

We can identify at least two categories of government-related issues in Internet fraud [and related computer crimes].

HARM TO GOVERNMENT. There are many examples of harm through Internet fraud to government. The principal and most serious threats include:

1. Espionage and theft of classified information;
2. Sabotage of vital government functions or services;
3. Anti-government dis-information and propaganda; and,
4. Penetration of government systems for the purpose of corrupting government decisions, including allocation of resources.

For the first class "Harm to Government" there is no point in estimating the value of the damage or the cost. All of the activities mentioned are well covered by Federal statutes or administrative practices. In addition, the government is well-staffed to protect its own interests since for all practical purposes it has almost unlimited manpower to counteract an Internet fraud should the occasion arise, e.g., if the damage or threat is great enough to merit a high level of attention.

CRIMINAL PROSECUTION. It is the government—Federal, State & Local—that is tasked with exacting the judicial compensation society demands for this type of damage. In addition to the "standard" use of incarceration, damages are composed of:

1. Monetary fines.
2. Punitive damages.[17]
3. Injunctive relief.

Generally, these punishments are determined by sentencing guidelines, containing fixed values. It appears that many fines are not calculated in relationship to the amount of damage, but rather are designed with end in mind of discouraging behavior.

Consequently, we can conclude that the entire class of damages from Internet fraud [and related computer crimes] as suffered by the government sector is not a relevant [useful] calculation [or estimation] to be made on a case-by-case basis.

---

[17] Usually imposed for willfully abusive behavior on the part of the convicted defendant.

B. Institutions [including Businesses] as Victim

In contrast, when an institution [including businesses] are seeking compensation, then estimating the value of damages is *crucial* to the outcome. See Table 1 at the end of this paper where we have divided the types of cost estimations into three categories based on their immediacy to the criminal event.

PRIMARY TIER. These are cost effects felt immediately upon occurrence of the Internet fraud. For example, the theft of property is immediate. [It is "gone" simultaneously with the event.]

For this type of loss, the cost estimation may be based on the *immediate replacement value* of the items [property] taken.

SECONDARY TIER. These cost effects are suffered *as an immediate consequence* of the Internet fraud [or related computer crime]. The most important among these is the "Reputational Effect," and as pointed out evidence indicates it can influence the stock market capitalization of the damaged victim firm.

Note that it is this effect and its possibly high *or even fatal* amount of damage that is at the root of the greatest executive fear, and explains the aversion to formal reporting [or other public disclosure] of any event.

TERTIARY TIER. Although virtually impossible to estimate, some thefts [or other Internet frauds] can cause long-term disruptions to the organization [or enterprise]. For example, the company might be completely precluded from entry into a market, thus losing potentially large amounts of revenue.

Due to the *essentially speculative nature* of these estimates [e.g., it is difficult to base the level of recoverable damages on a counting of future revenue that is only a possibility but not confirmed] we await a way to incorporate them into a grand tally of the cost of Internet fraud [and other related computer crimes].[18]

For all practical purpose, *it is not possible reasonably to estimate these costs.*

---

[18] This is very unfortunate, because the long-term effects of some Internet frauds are much more serious than are short-term effects, e.g., the company may be driven out of business.

C. *Individuals as Victim*

To most, horrible events in this category are criminal offenses involving homicide, soliciting, stalking, and sex crimes. The estimation of cost falls into the same category of anti-government [criminal] crimes, and thus is set not by calculation [or estimation] but by established schedules of penalties. In this context as well then, *it not relevant to make an estimation.*

However, for most crimes, there can be a civil tort complaint and the estimation of costs fall into the "classical" categories including (a) direct financial loss, (b) mental anguish, (c) damage to reputation, or (d) other types of damages associated with torts.

The rules governing tort recovery are more or less set and there is no need to review them here.

However, it should be added that it is likely that in contrast to institutions, individuals face generally severe and difficult hurdles achieving any compensation, and the standards required for showing of damages likely preclude real accommodation for the time and mental anguish spent in seeking compensation.

IV. CONCLUSION

This analysis suggests the following:

1. For criminal offenses, apart from punitive damages, the value of compensation for Internet fraud [and related computer crime] is fixed by sentencing [and other regulatory] guidelines; consequently, estimation of damages is not relevant.
    - NB: If such calculations were made for each event, they likely would differ substantially from agreed upon penalties.
2. For Internet fraud involving conversion of physical goods [e.g., inventory] or even most services, calculations of cost are straight forward, as they involve merely replacement or

substitution costs,
  - NB: Usually any associated *administrative* costs are added to these numbers as it represents the costs of making the replacement.
3. For compromise of intellectual property, including trade secrets, estimation of the costs is speculative in nature, since it must rely upon *forecasting* of how the property *probably would* benefit the victim in the future.
   - NB: The result is that the value is "calculated" likely will be the result of negotiations between the payer and payee.
4. For any use of external services [e.g., lawyers, accountants, consultants, forensic data services, investigators, etc.] the value of the harm is easily calculated by simply adding up the bills.
   - NB: The *opposite* is true for those resources expended internally. Usually companies fail to keep track of this,
   - NB: The *individual* equivalent of this would be the mental anguish and time wasted in cleaning up the mess left by an Internet fraud crime.
5. The consequent changes in (a) organizational behavior [or procedures], (b) re-engineering of security related procedures and infrastructure, are easy to calculate, because in more or less all organizations, these are done under a disciplined budgetary procedure. These expenditures can be very significant.

- NB: It is doubtful the bulk of these mandatory costs can be added to any damages award, and they are not reported in general computer crime statistics, but nevertheless they can be quite extensive, although "mixed" with other purposes.

Finally, it is important always to keep in mind the difference between (a) criminal penalties, (b) damage awards deriving from litigation, and (c) the true cost of Internet fraud [and related computer crime] which as you can see is likely much greater than either reported, or accounted for in litigation.

Table 1: Types of Cost Estimations for Internet Fraud [and Computer Related Crime]
Note: Use for Institutions and Individuals.

Type of Loss	Suggested Estimation
	PRIMARY TIER
Theft of Tangible Property	Value of Property + Administrative Costs of Recovery.
Theft of Services	Standard Value of Service if Purchased + Administrative Costs.
Theft of Trade Secrets	If in inventory, then use "book value" registered; if not recognized, then value is subject of negotiation.
	SECONDARY TIER
Reputational Effect	Negotiated valuation; drop in capital valuation of company; drop in reasonably expected sales.
Administrative Recovery Expenses	Cost of extra expenses associated with terminating and resolving the incidence, including: (a) legal costs, (b) investigative fees, (c) management time, and (d) other consulting and advisory fees.
	TERTIARY TIER
Competitive Displacement	Value of (a) permanent loss of market share, or (b) wind up value of company if driven out of business [by competition based upon using stolen trade secrets], or (c) estimation of opportunity cost for either (i) loss of geographical market, or (ii) inability to enter into new product line.

Security Administration (including Insurance)	Value of increased security costs [including additional insurance] compelled as a result of the Internet fraud incident including (a) staff turnover or extra hires, (b) re-engineering training and security awareness, and (c) purchase and operation of extra computer and network security infrastructure.

Source: Barraclough Legal Research

Table 2: Types of Internet Crime and Estimation of Losses

CRIME	ESTIMATION
ANTI-INDIVIDUAL CRIMES	
Murder, Negligent Homicide, Soliciting Suicide, Harassment, IIED, Stalking	No significant difference with same crimes not committed via Internet.
SEX CRIMES	
Soliciting a Minor, Corruption, Luring, Misuse of Personal Information on Minor, Sexual Harassment, Compelling Prostitution, Pimping	No significant difference with same crimes not committed via Internet.
OPERATIONAL HARM	
Spamming, Denial of Service Attacks, Vandalism, Release of Malware, Cybersquatting, Illicit Modification of Files, Falsification of Files.	Restoration costs, investigation and prosecution costs, loss of business, reputational loss, possible secondary losses to third parties.
MISUSE OF INTERNET	
Gambling, Selling Liquor or Cigarettes to Minors, Sale of illicit Prescription Drugs.	Covered by regular penalties and damages. No significant difference they are done via Internet.
INFRASTRUCTURE DAMAGE	
Computer Trespass, Malware (virus attacks), Destruction of Data, Modification or Corruption of Data, Denial of Service.	Cost of recovery & repair; Loss of Business; Reputational Loss; Change in Insurance Premiums.

FRAUD AND THEFT

Change credit rating; Embezzlement; Theft of Information; Theft of Services; Computer Impersonation; Pfishing; Theft of Goods; Theft of Money.	For Theft of goods and services, use market value; for change of credit rating, use value difference in additional credit obtained; For Impersonation, estimate damages caused [no damages if act had no result]. It is necessary to estimate the *secondary effects* of loss [e.g., missuse] of personal name-linked information.

ANTI-GOVERNMENT CRIMES

Obstruction, Failure to Report, False Reporting, Tampering with Evidence, Endangering Public Safety	Use accepted criminal penalties. No significant difference because crimes committed with Internet.

THEFT OF INTELLECTUAL PROPERTY

Stealing of Patents; Improper use of Copyrighted Material; Theft of Trade Secrets.	For patent infringement, use standard remedies and values. Same for Copyrighted materials that are taken. For Trade Secrets, it is problematical to assign a value since (1) values may change over time, (2) many valus are of necessity "speculative" in nature.

Based on the Model Computer Crime Code

TECHNOLOGY, STALKING AND DOMESTIC VIOLENCE VICTIMS

Cindy Southworth and
Sarah Tucker[*]

The Digital Age is bringing many opportunities to survivors of abuse and their advocates.[1] Across America, victims of domestic violence are using the revolutionary tool of the Internet to map roads to new lives by reaching out to shelters, researching restraining orders, and finding housing and employment opportunities. However, at the same time, advancements in technology are posing unique challenges to enhancing victim safety. Abusers regularly use a variety of technologies to stalk current and former intimate partners, ranging from phones to mapping to computer technologies. Some abusers install global positioning systems to stalk their victim's real-time locations with extraordinary accuracy, while others use telephones to leave hundreds of messages in a single day. Other stalkers use technologies like caller ID during a relationship to monitor their partner's calls, and to locate her after she has fled. Still others use online databases, electronic records, and web search engines to locate, track, and harass former partners. Regardless of the tool or technology used, perpetrators have the same primary goal: abusing power to gain and maintain control over their victims.

---

[*] Safety Net: the Safe and Strategic Technology Project at the National Network to End Domestic Violence Fund

[1] Since people surviving abuse identify themselves differently, in this article the terms "victim" and "survivor" are used interchangeably. "Stalker," "abuser" and "offender" are also used interchangeably to reference perpetrators of intimate partner violence — a category encompassing domestic violence, sexual violence, and stalking that targets a current or former spouse, boyfriend, girlfriend, or significant other. LAWRENCE A. FREENFELD, ET AL., U.S. DEP'T OF JUSTICE, NCJ-167237, VIOLENCE BY INTIMATES: ANALYSIS OF DATA ON CRIMES BY CURRENT OR FORMER SPOUSES, BOYFRIENDS, AND GIRLFRIENDS, at iii (1998), available at http://www.ojp.usdoj.gov/bjs/pub/pdf/vi/pdf (last visited January 29, 2007).

I. COMPUTER & INTERNET TECHNOLOGY

Abusers continue to identify and adapt new computer software and hardware tools that allow them to further stalk and harass their victims. They not only use low-technology monitoring options such as viewing the website browser history or intercepting email, but also are increasingly using more sophisticated SpyWare software and hardware for surveillance.

A. Computer Monitoring Software and Hardware

In September 2001, a Michigan man was charged with installing spy software on the computer of his estranged wife. Without her knowledge, a SpyWare program sent him regular emails reporting all of her computer activity, including all emails sent and received and all web sites visited.[2]

Computer monitoring software, or "SpyWare", was originally developed to monitor children's Internet use, but has also been utilized by abusers. It allows an abuser to monitor computer and Internet activities and discover a victim's efforts to escape or access help. This software can be installed remotely or by physically accessing the victim's computer. One man admitted that he "e-mailed his ex-wife Spyware that automatically downloaded to her computer, which allowed him to secretly monitor her online communications and read her e-mail."[3]

Although SpyWare detection programs claim to uncover the hidden SpyWare programs, they are imperfect in their counter surveillance. "Scrubber" and "washer" programs that claim to clear computer histories are ineffective if SpyWare is in use. Additionally, if the victim installs new programs or clears all computer trails, this could cause suspicion and increase danger.

---

[2] Mike Wendland, *State Targets Cyber Spies: Belleville Man Accused of Electronic Voyeurism*, DETROIT FREE PRESS, Sept. 6, 2001 at 1B.

[3] TheKansasCityChannel.com, *Gladstone Man Pleads Guilty to Cyber-Stalking*, Aug. 25, 2005, http://www.thekansascitychannel.com/news/4898760/detail.html (last visited Feb. 1, 2007).

Spyware is not just for desktop and laptop computers anymore. As more and more people are using cell phones or handheld devices to access the Internet, spy software has kept up with this trend. In March of 2006, Vervata began advertising FlexiSpy which "captures call logs, text messages and mobile Internet activity, among other things."[4] It sells for $49.95 and is advertised "as a tool to monitor kids and unfaithful spouses."[5]

In additional to software programs, stalkers use hardware devices called "Keystroke Loggers" that are inserted into a USB port or between the keyboard cable and the back of the computer. These tiny devices contain small hard drives that record every key typed, including all passwords, Personal Identification Numbers (PIN), websites, and email. However, abusers must have physical access to a victim's computer in order to use these devices, as they must physically retrieve the information stored on them.

B. *The Internet*

"A police officer seeking revenge against a former girlfriend hacked into the woman's e-mail account, assumed her identity at an online dating service and contacted 70 men, inviting some of them for rendezvous at the woman's home."[6] Another abuser changed his wife's email password and sent threatening messages to himself from her email account. Then he took the printed messages to the police and asked them to arrest her. Another abuser discovered that his victim was planning to flee by viewing an email she thought she had deleted. However, she did not realize that she had to empty her "deleted items" folder. He discovered her escape plan by checking this folder, and he killed her.[7]

---

[4] Joris Evers, *Spy Program Snoops on CellPhones*, CNET NEWS.COM, Mar. 29, 2006, http://news.com.com/spy+program+snoop+on+cell+phones/2100-1029_3-6055760.html (last visited Feb. 1, 2007).

[5] *Id.*

[6] Erik German, *Officer Charged with Cyber-Stalking His Ex*, L.A. TIMES, Apr. 4, 2006, at A19.

Stalkers are setting up websites that threaten victims or encourage others to contact, harass, or harm the victim. Some abusers encourage others to stalk their victim by posting erroneous and harassing information on websites (e.g. that the stalker's ex-wife enjoys being raped). In one scenario, an abuser had his parental rights terminated when his child was a toddler. Years later he posted a very old family photograph and details about his then ten-year-old child. The mother and child were terrified to discover the presence and content of this website.[8]

Stalkers use free and fee-based websites to track private information about their victims. Information brokers are commercial entities that buy and sell data, and frequently acquire information from public records and retail databases. In addition to fee-based services, many free websites such as court databases, voter registration, and religious directories provide a wealth of private contact information that can be used to track survivors nationwide as they attempt to relocate. Many courts are beginning to publish both indexes of court records and the full documents and case files to the Internet, often without providing any notice to citizens or options for victims to restrict web-access. A Montgomery County, Pennsylvania Court went a step further, publishing the names and addresses of victims (and their children) who obtain protection orders to the web.[9]

The mere existence of a victim's name on a website could lead a batterer or stalker to a victim's new community, if not her exact address. If a victim moves to a new town to start a new life away from a batterer, she might be found if an online court index lists only her name on the Internet. Failing to expressly exclude victim and witness identities from web or remote access will mark these victims and witnesses for continued violence and harassment by the batterer. This encroachment on privacy and the resulting threat to personal safety will discourage victims of domestic violence from seeking protection from their abusers, just as it will discourage witnesses from helping to end the violence through their testimony.

---

[7] CINDY SOUTHWORTH ET AL., NAT'L NETWORK TO END DOMESTIC VIOLENCE, A HIGH-TECH TWIST ON ABUSE: TECHNOLOGY, INTIMATE PARTNERS STALKING, AND ADVOCACY 8 (2005), *available at* http://www.mincava.umn.edu/documents/commissioned/stalkingandtech/stalkingandtech.pdf.

[8] *Id.*

[9] Katharine Webster, *Victim Advocates Want Names, Addresses, Records Offline*, USA TODAY ONLINE, Dec. 1, 2003, http://www.usatoday.com/tech/news/internetprivacy/2003-12-01-victim-privacy_x.htm (last visited Feb. 1, 2007).

Most public filings can give abusers the information they need to track their victims. Posting such filings on the Web increases their utility and accessibility for some, but also increases the chance that victims will be found. For example, if a victim of domestic violence flees her abuser in Virginia, relocates to Texas, buys property, and files her land record with a court that posts such records on the Web, her abuser can find her with a simple, national HTML search. Many of life's most important events involve the court system. In a jurisdiction where the court posts records on the Internet, a victim of domestic violence must weigh the benefits of the activity against the possibility that her attacker will locate her.

C. Location & Surveillance Technologies

> I've been tracking my girlfriend through her mobile phone. I can see exactly where she is, at any time of day or night, within 150 yards, as long as her phone is on. . . . . On the website, I see the familiar number in my list of "GSM devices" and I click "locate". A map appears of the area in which we live, with a person-shaped blob in the middle, roughly 100 yards from our home. . . . . There is no trace of what I'm doing on her phone. . . . . I can't find anything in her mobile that could possibly let her know that I'm checking her location. As devious systems go, it's foolproof. I set up the website to track her at regular intervals, take a snapshot of her whereabouts automatically, every half hour, and plot her path

> on the map, so that I can view it at my leisure.[10]

Although Goldacre had his girlfriend's permission to track her for an article he wrote, his account illustrates how incredibly easy it is to track someone via their cell phone signal or a GPS chip. Before abusers had access to location tracking devices like global positioning systems, they often checked car odometers to measure mileage and monitor victims' daily activities. Now, abusers can track their victims with Global Positioning Systems (GPS) that use satellite receivers to provide precise real-time worldwide positioning. These devices vary by price, size, and appearance, ranging from a small black box to a hand-held unit to a small chip in a wristband. In December 2002, a Wisconsin man secretly installed a GPS device under the hood of his ex-girlfriend's car and stalked her for months. "He would follow her as she drove to work or ran errands. He would inexplicably pull up next to her at stoplights and once tried to run her off the highway . . . .[11] Since 2002, GPS systems have become less expensive and many are being marketed as ways for parents to track their teen drivers. The lower cost and increased availability has made them available to more of the general public, stalkers included. This may be one reason for the sharp increase in the number of GPS stalking cases reported by the media in recent years.

While many cell phones now have GPS chips in them to aid 911 operators in identifying their location, older phones do not. Yet, these can still be located. A variety of services operate on the Internet, offering to locate a phone though the cell towers it is accessing or through an internal GPS chip, often using illegal means to provide this information to anyone willing to pay.

---

[10] Ben Goldacre, *Short Cuts: How I Stalked My Girlfriend*, THE GUARDIAN (LONDON), Feb. 1, 2006, at 2.

[11] Kevin Orland, *Stalker Victims Should Check for GPS*, CBS NEWS.COM, Feb. 6, 2003, http://www.cbsnews.com/stories/2003/02/06/tech/main539596.shtml (last visited Feb. 1, 2007).

D. Cameras

Stalkers use small hidden cameras to monitor their victims and learn their routines. Small wireless high-resolution cameras can be hidden in smoke detectors, children's lamps, or behind a pin-sized hole in a wall, and can even be activated remotely. In 2003, the Supreme Court of New Jersey found that a defendant's video surveillance of his estranged wife in her bedroom presented a prima facie case of stalking and harassment under the New Jersey Domestic Violence Act.[12]

As web cameras become increasingly popular, these too are being used by perpetrators. With the recent increases in the use of high-speed Internet service, many people are using an "always on" Internet connection.[13] As if they weren't scary enough, many spyware programs also allow a user to remotely activate a webcam, allowing an abuser to turn on the camera at anytime, using it as a window into the living room of the victim.

II. PHONE TECHNOLOGY

While technology has greatly enhanced our ability to communicate by providing us with a wide variety of newer and better tools, telephones remain the one of most prevalent and least expensive communication technologies. Because of this, many abusers rely on telephones as their first weapon to harass their victims, through repeated and harassing phone calls or threatening messages left in voicemail and on answering machines.

While harassing calls made using a traditional land line telephone (vs. a cellular phone) can be traced via phone company records, there's no guarantee that the phone at the other end will have any connection to the perpetrator. It could be at a friend's home, hotel, or even a pay phone at the local gas station. Until recently, tracing cell or wireless phone calls has been somewhat easier as these phones generally belong to an individual and have a credit card number and address associated with them. However, the advent of pre-paid phones has made this increasingly difficult. If a phone card or prepaid cell phone is not activated with a credit card, linked to a discount card, or billed to a person's long distance phone carrier, the harassing call can be more difficult to trace.

---

[12] *See* H.E.S. v. J.C.S., 815 A.2d 405, 415-17 (N.J. 2003).

[13] JOHN B. HORRIGAN, PEW INTERNET & AMERICAN LIFE PROJECT, HOME BROADBAND ADOPTION 2006 (May 28, 2006), *available at* http://www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf.

A. Caller ID

Most cell phones and many Caller ID enabled phones keep an internal record of incoming and outgoing calls, which abusers often use to monitor survivors' phone use. In Rhode Island, one abuser assaulted his wife after finding the shelter phone number in her cell phone call history; as a result she did not attempt to leave her husband for another year.[14] Caller ID also allows abusers to stalk and locate their victim after the relationship has ended. Soon after Caller ID was first available, an abuser in Texas used Caller ID to track down his former girlfriend and murdered her.[15]

B. Fax Machines

Abusers and stalkers have used the fax header on faxed documents to locate their victims. In one example, a woman fled, but had to send papers to her abusive partner. She faxed the papers from the shelter fax machine to her attorney. Her attorney faxed the papers to his attorney. His attorney gave the papers to him. Since no one removed the fax header, the abuser acquired the phone number and location of his victim and she had to relocate again.[16]

---

[14] SOUTHWORTH, *supra* note 7, at 6.

[15] Associated Press, *Man Charged in Caller ID Killing*, DALLAS MORNING NEWS, Mar. 30, 1995, at A33.

[16] SOUTHWORTH, *supra* note 7, at 6.

C. *TTY/TTD*

Teletypewriters (TTY) and Telecommunications Devices for the Deaf (TTD) are text based phones that people who are deaf or hard of hearing use to communicate. These devices often record and save an exact history of conversations, making it easier for stalkers to monitor victims' conversations. Abusers also impersonate victims by using their TTY to seek information about their activities. In one case, a prosecutor working with a deaf victim got a call on his TTY, allegedly from the victim, reading, "If you don't drop the charges against my boyfriend, I'm going to kill myself." When help was sent to the victim's home it emerged that she had been sleeping when the TTY call was made. The abuser had impersonated the victim in an attempt to persuade the prosecutor to withdraw charges.[17]

III. CONCLUSION

As devices continue to meld, the distinctions currently made between computers, phones, fax machines, cameras, and TTYs are quickly disappearing. Many handheld devices allow the user to search the Internet, send instant messages, take photos, and send text messages. Some people use web cameras and online chat websites (like AOL's AIM) to simultaneously text message and view others. Emerging technologies like VoIP, a popular method of cheap long distance phone via the Internet, further blur a user's sense between phone and online communication. The recent increase in the popularity of chat rooms, forums, and blogs has been evident too, as more survivors use these as vehicles to share their stories and seek support. All of these technologies are also increasingly used by abusers to harass, deceive, monitor, and stalk survivors.

As stalkers continue to increase their use of technology, it is vital that communities are equipped to respond to these crimes. In an age where stalkers use search engines to track them down, victims need to be able to relocate safely. As more records are published on the Internet, advocates must educate community agencies, courts, and government offices about the potential dangers to victims and the importance of notification and privacy options. When electronic evidence is needed to prosecute a crime, advocates can work to ensure that specialized violence against women law enforcement and prosecution units receive additional training or access to a technology crime unit. Whether working within the legal system, community social services, or with other civic organizations, education and ally building are critical to lessening the barriers that victims of technology stalking encounter.

---

[17] *Id.*

While much is unknown about the future of technology and the emerging uses of technology in intimate partner stalking, advocates and allies must continue to press on learning, educating, and advocating for change. Intimate partner stalkers are persistent and resourceful, but so are the advocates and survivors fighting against them.

CHILD PORNOGRAPHY AND FIRST AMENDMENT STANDARDS

Kyle Duncan[*]

This paper explains how the Supreme Court currently applies the First Amendment to laws targeting child pornography. In light of those standards, the paper explores some current areas in child pornography law, principally Congress's legislative response to the Supreme Court's decision in *Ashcroft v. Free Speech Coalition*[1] regarding "virtual" child pornography. The purpose of this paper is primarily descriptive, rather than evaluative, but it does offer some criticisms of these judicial and legislative approaches to the continuing and distressing problem of child pornography. Part I explains the Supreme Court's general approach—known as "categorical balancing"—to defining areas of expression that are withdrawn from the full protection of the First Amendment. Part I then places child pornography within that analytical framework. Part II moves to the most current area of child pornography law—"virtual" child porn—and discusses how the Supreme Court addressed Congress's efforts to combat that problem in the 2002 Ashcroft decision. It then discusses Congress's response to *Ashcroft* in the 2003 amendments to federal child pornography laws. Part III concludes the paper by discussing how the state and lower federal courts have addressed issues posed both by *Ashcroft* and the amended federal law.

---

[*] Assistant Professor of Law, University of Mississippi School of Law. I am grateful to the National Center for Justice and the Rule of Law for their generous financial support during the preparation of this paper.

[1] 535 U.S. 234 (2002).

I. From Inciting Crime to Exploiting Children: How the Supreme Court Identifies Unprotected Expression

Because all speech cannot be free, it seems inevitable that the Supreme Court must police the constitutional boundaries of "free speech." But that practice, in and of itself, presents an irresolvable contradiction. This is not merely the problem that the First Amendment speaks in absolute terms ("Congress shall make no law . . ."), but the deeper problem of content selection. We have been conditioned, correctly, to regard government punishment of particular messages with the darkest suspicion. When the state suppresses certain ideas *because* of their content—and lets other, "approved" ideas freely circulate—we sense the sinister hand of censorship striking, not merely at our liberties, but at the very sources of self-government, freedom, and personality. And yet the Supreme Court itself not only engages in such a practice, but freely admits it to be the foundation of its Free Speech jurisprudence. When the Court says "this expression is outside First Amendment protection, but *this* is in," it is doing nothing other than selectively allowing the suppression of certain expressive messages. To confirm this impression, let us hear the Court speak for itself:

> The First Amendment generally prevents government from proscribing speech, or even expressive conduct, because of disapproval of the ideas expressed. Content-based regulations are presumptively invalid. From 1791 to the present, however, our society, like other free but civilized societies, has permitted restrictions upon the content of speech in a few limited areas, which are "of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality." We have recognized that "the freedom of speech" referred to by the First Amendment does not include a freedom to disregard these traditional limitations. Our decisions since the 1960's have narrowed the scope of the traditional categorical exceptions for defamation, and for obscenity, but a limited categorical approach has remained an important part of our

First Amendment jurisprudence.[2]

That the absolutist Free Speech Clause turns out to be non-absolute should neither surprise nor disturb. The Court tells us that all "free but civilized societies" allow such adjustments to free speech. It must be so: anyone claiming free rein for malignant speech like defamation or solicitation of murder would brand himself a lunatic (or a tenured law professor). But not all "free but civilized societies" have decreed that such adjustments be made by *courts*. Two centuries ago no less a figure than Alexander Hamilton predicted that attempting to liquidate the precise boundaries of phrases such as "liberty of press" was a fool's errand.[3] In fact, Hamilton suggested heretically (by our modern standards) that the "security" of such expressive liberty, "whatever fine declarations may be inserted in any constitution respecting it, must altogether depend on public opinion, and on the general spirit of the people and of the government."[4] The extent of our liberties, therefore, would be sketched out through "legislative discretion, regulated by public opinion."[5] Hamilton had a point about the difficulty of judicially delineating the boundaries of free speech, but we have nonetheless asked modern courts to try. This is an instructive backdrop to understanding the Court's attempts to describe "categories" of expression that are outside the central precincts of the First Amendment.

---

[2] R.A.V. v. City of St. Paul, 505 U.S. 377, 382-83 (1992) (citations omitted). Relevant to our purposes here, the Court added, by way of comfort, that "these areas of speech can, consistently with the First Amendment, be regulated because of their constitutionally proscribable content (obscenity, defamation, etc.)—not that they are categories of speech entirely invisible to the Constitution, so that they may be made the vehicles for content discrimination unrelated to their distinctively proscribable content. Thus, the government may proscribe libel; but it may not make the further content discrimination of proscribing only libel critical of the government. We recently acknowledged this distinction in *Ferber*, where, in upholding New York's child pornography law, we expressly recognized that there was no 'question here of censoring a particular literary theme . . . .'" *Id.* at 383-84.

[3] In Federalist 84, Hamilton asked derisively, "What is the liberty of the press? Who can give it any definition that would not leave the utmost latitude for evasion? I hold it to be impracticable. . . .]" THE FEDERALIST NO. 84, at 446 (Alexander Hamilton) (George Wescott Carey et al. eds., 2001).

[4] *Id.*

[5] *Id.*

The most celebrated category has been the most difficult of all to nail down. In a series of early-to-mid 20th century decisions made famous by Holmes's and Brandeis's dissents, the Court unconvincingly struggled to define a category of speech that was unprotected because of its propensity to encourage law-breaking.[6] This is a kind of speech that lives in the shadows of vivid metaphors—"clear and present danger," "shouting 'fire' in a crowded theater"—but that eludes categorical definition. The Court finally settled on a highly speech-protective formulation in *Brandenburg v. Ohio*, allowing suppression only when speech incites imminent law-breaking that is also likely to imminently occur.[7] It is, of course, unclear how "imminent" the law-breaking must be, how clear the intent to incite must appear from the speaker's words (or actions), or even whether the threatened law-breaking must be "serious." Further, it is quite alarming to imagine the *Brandenburg* standard applying to the solicitation of murder. In this age of radical Islamist incitement to violence, disguised as religious speech, many harder questions about the scope of *Brandenburg* likely will arise. But beyond the difficulties of definition, it is important for our purposes to recognize the sensible motivation behind regulating this speech. Incitement to immediate law-breaking short circuits the usual remedies for bad speech, because it eliminates the possibility of counter-speech. Such speech does not seek to exchange ideas or further political consensus. Indeed, such speech is the antithesis of political speech because it seeks to subvert the political process altogether.

The specter of violence also led the Court to define two other areas of unprotected speech: "fighting words" and "true threats." These are first cousins to *Brandenburg* speech, but present subtly different dynamics. Fighting words, for instance, threaten not merely imminent law-breaking but rather violence against the speaker himself. They refer to abusive face-to-face language calculated, or perhaps only likely, to evoke an immediate retaliation against the speaker.[8] The nature and circumstances of the speech make it more like a slap in the face—or as John Hart Ely wrote, an "unambiguous invitation to a brawl"[9]—and less like an invitation to exchange ideas. In other words, fighting words are not looking for counter-speech, but for counter-violence. The Supreme Court has not upheld a conviction based on the fighting words rationale since *Chaplinsky* in 1947, so it is unclear how this doctrinal category has been influenced by the Court's subsequent development of the incitement category, or whether this category is entirely separate.

---

[6] *See, e.g.*, Whitney v. California, 274 U.S. 357 (1927); Gitlow v. New York, 268 U.S. 652 (1925); Abrams v. United States, 250 U.S. 616 (1919); Debs v. United States, 249 U.S. 211 (1919); Schenck v. United States, 249 U.S. 47 (1919).

[7] 395 U.S. 444 (1969).

"True threats" are words that are intended to place, and actually do place, someone in fear that force or violence will be used against them.[10] Such expression is outside the First Amendment because it engenders fear in the recipient, altering his behavior and perhaps promoting retaliation. In *Virginia v. Black*—a case about cross-burning—the Court was willing to disassociate the harm posed by this symbolic threat from the racist ideology historically intertwined with it.[11] On this view, the Court would likely have approved Virginia's singling out of cross-burning as a "virulent" form of symbolic threat, had the Court not struck down the law for other reasons.[12] This should be contrasted with the Court's treatment of virulent fighting words in *R.A.V. v. City of St. Paul.*[13] There, the Court was unwilling to detach the ideology of racist, religious or other epithets from their heightened propensity to cause fights. Unlike in *Black*, the *R.A.V.* Court invalidated the law as a form of viewpoint discrimination against certain ideologies. The difference between *Black* and *R.A.V.* is hard to justify, although it may turn on the difference between threats and fighting words, or perhaps on the differences between symbols and purely verbal expression.

---

[8] *See* Chaplinsky v. New Hampshire, 315 U.S. 568 (1942).

[9] JOHN HART ELY, DEMOCRACY AND DISTRUST 114 (1980).

[10] *See* Virginia v. Black, 538 U.S. 343, 359-60 (2003).

[11] *See id.* at 361-63.

[12] *See id.* at 363-67 (plurality op.).

[13] 505 U.S. 377, 391-95 (1992).

But looming violence is not the only reason the Court has singled out unprotected areas of speech. The Court's treatment of "obscenity" takes us one step closer to the problem of child pornography, and so it is worth understanding precisely why the Court allows government greater latitude for regulating obscene expression. The Court originally approved the exclusion of obscenity from the First Amendment strictly on the grounds that such limitations were widely embraced by the framing generation.[14] Since then, the Court has had to refine its understanding of what, precisely, constitutes unprotected obscene expression. This has not been easy, evidenced by the fact that, for several years, the Court could not agree on a standard and simply reversed and remanded cases when five justices, applying their own standards, deemed allegedly obscene materials protected.[15] With *Miller v. California*[16] in 1973, however, the Court finally achieved majority consensus. Under the Miller standard, the government may regulate materials as "obscene" only if a trier of fact, under authoritatively interpreted state law, finds that (1) the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; (2) the work depicts or describes, in a patently offensive way, sexual conduct specifically described by the applicable state law; and (3) the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[17] Unsurprisingly, this Byzantine definition raises as many questions as it answers. The Court has since clarified that (1) *local* community standards determine prurience and patent offensiveness, as opposed to state or national standards;[18] (2) jury verdicts, however, are subject to judicial review to guard against "constitutionally aberrant" determinations of local community standards;[19] and (3) the presence *vel non* of serious content is not governed by local community standards, but rather by a reasonable person standard.[20] Finally, in *Miller* itself, the Court provided a rather embarrassing sampling of the activities state law may deem "patently offensive" sexual depictions—confirming the impression that the *Miller* Court had in mind pornography of the "hard core" variety.[21]

---

[14] Roth v. United States, 354 U.S. 476, 482-83 (1957).

[15] *See, e.g.*, Redrup v. New York, 386 U.S. 767 (1967).

[16] 413 U.S. 15 (1973).

[17] *Id.* at 25.

[18] Hamling v. United States, 418 U.S. 87 (1974).

Why is obscene expression withdrawn from First Amendment protections? The overriding state interest articulated in *Miller* is avoiding offending the sensibilities of unwilling recipients and exposure to juveniles.[22] But in a companion case, *Paris Adult Theater I v. Slaton*,[23] the Court articulated a wider range of state interests in combating obscenity. The Court recognized the public's interest in "the quality of life and the total community environment, the tone of commerce in the great city centers, and, possibly, the public safety itself."[24] More strikingly, the Court suggested that a state might conclude that "commerce in obscene books, or public exhibitions focused on obscene conduct, have a tendency to exert a corrupting and debasing impact leading to antisocial behavior."[25] The Court explicitly rejected the notion that the state's interest was confined to ensuring that the traffic in obscenity was based on the participating adults' consent. It remains to be seen whether this language from *Paris Adult Theater I* survives more recent decisions of the Court that constitutionalize the notion of consenting adults' privacy in both reproductive and non-reproductive sexual matters.[26]

---

[19] Jenkins v. Georgia, 418 U.S. 153 (1974).

[20] Pope v. Illinois, 481 U.S. 497 (1987); Smith v. United States, 431 U.S. 291 (1977).

[21] *Miller*, 413 U.S. at 25. A few additional nuances of obscenity law should be noted. Prior to *Miller*, the Court had held that the state may not criminalize the private possession of even legally obscene material. *Stanley v. Georgia*, 394 U.S. 557 (1969). But notwithstanding *Stanley*, the Court allows states to criminalize the importation and interstate transportation of obscene materials, even if destined for purely private use. *See* United States v. Twelve 200-Foot Reels of Super 8mm Film, 413 U.S. 123 (1973); United States v. Orito, 413 U.S. 139 (1973); United States v. Riedel, 402 U.S. 351 (1971).

[22] *Miller*, 413 U.S. at 18-19.

[23] 413 U.S. 49 (1973).

[24] *Id.* at 58.

[25] *Id.* at 63.

When turning to the First Amendment law of child pornography, it should be underscored that the Supreme Court has chosen to address this area as doctrinally distinct from the category of obscenity. The Court discerns a conceptually different harm posed by the materials themselves, and consequently recognizes a distinct state interest in regulating the expression. There is much to be said for this approach, but it should be said that there is something artificial about it. Child pornography and hard-core pornography are not distinct categories of expression; they are close neighbors in the same lurid neighborhood. The fact that the Court has elected to treat them as separable doctrinal categories should not obscure the fact that employing children in pornography remains a particularly sickening subgenre of an already diseased field. This becomes relevant later in the paper, for where the doctrinal tools of child pornography law prove inadequate, the government can, and has, turned to the category of obscenity for an alternative mode of attack.

In a 1982 decision, *Ferber v. New York*, the Supreme Court held that a state may criminalize visual depictions of sexual conduct involving minors that would not otherwise meet the *Miller* obscenity standard.[27] The state would, of course, have to adequately define the prohibited conduct. In *Ferber*, the Supreme Court approved a New York law that criminalized the "promotion" of a "sexual performance" by a child less than 16 years old.[28] It is worth underscoring precisely how the *Ferber* standard departs from the *Miller* obscenity standard. As the Court explained, with regard to child pornography, *Ferber* "adjusts" *Miller* as follows:

---

[26] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003); Planned Parenthood of S.E. Pa. v. Casey, 505 U.S. 833 (1992).

[27] 458 U.S. 747 (1982).

[28] *Id.* at 750-51. A *performance* was defined as "any play, motion picture, photograph or dance" or "any other visual representation exhibited before an audience." *Id.* at 751 (quoting N.Y. PENAL LAW § 263.00(4)). A *sexual performance* was defined as "any performance or part thereof which includes sexual conduct by a child less than 16 years of age." *Id.* (quoting § 263.00(1)). In turn, *sexual conduct*

> [1] A trier of fact need not find that the material appeals to the prurient interest of the average person; [2] it is not required that the sexual conduct portrayed be done so in a patently offensive manner; and [3] the material at issue need not be considered as a whole.[29]

What are the distinct reasons for which child pornography is unprotected by the First Amendment? First and foremost, the state has a compelling interest in safeguarding the physical and psychological well-being of minors—more precisely, in safeguarding minors from being "subjects of pornographic materials."[30] By contrast, *Miller* had identified no state interest in the adult performers' physical, moral, or psychological welfare. Second, the distribution network for child pornography may be closed, both to prevent further harm to the subject children caused by circulation of the "permanent record of [their] participation," and also to choke off the market for the pornography.[31] Third, the state could strike at the economic drivers—advertising and selling—of the pornography.[32] Finally, the Court asserted that any serious literary, scientific, or educational value from such depictions is virtually non-existent:

> [I]f it were necessary for literary or artistic value, a person over the statutory age who perhaps looked younger could be utilized . . . . Nor is there any question here of censoring a particular literary theme or portrayal of sexual activity. The

---

was defined as "actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals." *Id.* (quoting § 263.00(3)). Under the New York law, *promotion* of a child sexual performance means "to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmute, publish, distribute, circulate, disseminate, present, exhibit or advertise, or to offer or agree to do the same." *Id.* (quoting § 263.00(5)).

[29] *Id.* at 764.

[30] *Id.* at 757-59.

[31] *Id.* at 759-60.

[32] *Id.* at 761-62.

> First Amendment interest is limited to that of rendering the portrayal somewhat more "realistic" by utilizing or photographing children.[33]

Subsequently, the Court held that, unlike garden-variety obscenity, the state may criminalize the *private possession* of child pornography.[34]

II. VIRTUAL AND SIMULATED CHILD PORN: THE CONVERSATION BETWEEN CONGRESS AND THE COURT

The standard federal definition of child pornography tracks the boundaries set out in *Ferber*.[35] In 1996, however, Congress broadened federal law to strike at the phenomena of so-called "virtual" and "simulated" child porn by passing the Child Pornography Prevention Act of 1996 (the "CPPA").[36] In 2002, the Supreme Court invalidated parts of the CPPA in *Ashcroft v. Free Speech Coalition*.[37] The paper will discuss the CPPA in terms of the *Ashcroft* decision.

A key provision of the CPPA prohibited "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture" that "is, *or appears to be*, of a minor engaging in sexually explicit conduct."[38] As discussed below, this provision was struck down by *Ashcroft*, and has been rewritten by the 2003 amendments to the CPPA.[39] Another CPPA provision struck down by *Ashcroft* was one prohibiting any sexually explicit image that was "advertised, promoted, presented, described, or distributed *in such a manner that conveys the impression*" it depicts "a minor engaging in sexually explicit conduct."[40] This section was dropped from the law in the 2003 revision. The *Ashcroft* Court did not address (because it was not challenged) the CPPA provision prohibiting child pornography through "computer morphing," defined as visual depictions that were "created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."[41] Why did *Ashcroft* invalidate the "appears to be" and "conveys the impression" provisions of the CPPA? Understanding that will clarify the current limits placed by the First Amendment on child pornography law.

---

[33] *Id.* at 763 (citation omitted).

[34] Osborne v. Ohio, 495 U.S. 103 (1990).

[35] *See, e.g.*, 18 U.S.C. § 2252(a)(1)(A) (2000) (criminalizing transport of a "visual depiction involv[ing] the use of a minor engaging in sexually explicit conduct"). For an informative summary of the federal government's legal efforts to combat child pornography, see the Eleventh Circuit's discussion in *United States v. Williams*, 444 F.3d 1286 (11th Cir. 2006).

[36] *See generally* Child Pornography Prevention Act of 1996, 18 U.S.C. §§ 2251-2260 (2000 & Supp. 2003).

[37] 535 U.S. 234 (2002).

[38] 18 U.S.C. § 2256(8)(B) (2000), *amdended by* 18 U.S.C. 2256(8)(B) (Supp. 2003) (emphasis added).

[39] *See* § 2256(8)(B) (now defining "visual depiction" as "a digital image, computer image, or computer-generated image that is, or *is indistinguishable from*, that of a minor engaging in sexually explicit conduct" (emphasis added)). For the

The *Ashcroft* majority (Kennedy, with Stevens, Souter, Ginsburg and Breyer) focused most of its analysis on the "appears to be" provision. In striking it down, the majority emphasized that the CPPA went well beyond the *Miller* obscenity standards because it banned materials without regard to whether they appealed to the prurient interest, whether they depicted sexual activity in a patently offensive manner, whether they had any serious value, and (implicitly) whether the works were considered "as a whole."[42] The majority also reasoned that the provision detached the CPPA from the unique state interests at stake in *Ferber*—which targeted "speech that itself is the record of sexual abuse"—because the CPPA "prohibits speech that records no crime and creates no victims *by its production.*"[43] The majority was concerned that, because the "appears to be" provision was divorced from both *Miller* and *Ferber*, it could sweep into its coverage genuine literary works that depict "an idea—that of teenagers engaging in sexual activity—that is a fact of modern society and has been a theme

---

rationale behind these and other changes to the law, see H.R. REP. NO. 108-66, at 31 (2003) (Conf. Rep.), *as reprinted in* 2003 U.S.C.C.A.N. 683, 695, especially the findings in section 502. These matters are discussed below.

[40] § 2256(8)(D) (repealed 2003) (emphasis added).

[41] § 2256(8)(C).

[42] *Ashcroft*, 535 U.S. at 240

[43] *Id.* at 250 (emphasis added).

in art and literature throughout the ages."[44] The Court was particularly exercised over the prospect of the CPPA criminalizing Baz Luhrmann's film version of *Romeo and Juliet*, and the Academy Award-winning films *Traffic* and *American Beauty*.[45]

The majority was not receptive to the government's arguments that the CPPA properly banned "virtual" child pornography because such material provided tools for pedophiles to seduce children, or because they "whet people's appetite" for actual child pornography. The majority reasoned that "[t]he mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it."[46] Exploiting a connection between virtual child pornography and actual child sexual abuse would require, in the majority's view, a much closer link (one presumably on the order of *Brandenburg*-type "incitement").[47] Nor did the majority accept the argument that, because the virtual images were "indistinguishable" from real images, the two kinds of images were part of the same "market" and thus required a blanket ban. The majority called this argument "somewhat implausible" because, it thought, "[i]f virtual images were identical to illegal child pornography, the illegal images would be driven from the market by the indistinguishable substitutes."[48] No one would risk producing real child pornography, the majority reasoned, if "fictional, computerized images would suffice."[49]

Finally, the majority rejected the argument that indistinguishable virtual images made prosecution of genuine child pornography difficult because "[e]xperts . . . may have difficulty in saying whether the pictures were made by using real children or by using computer imaging."[50] The majority thought this argument "turn[ed] the First Amendment upside down" by calling for the banning of protected speech to further the suppression of unprotected speech.[51] A premise of Free Speech doctrine, said the Court (pointing to the overbreadth doctrine as an example), was that even unprotected speech could not be banned if a substantial amount of protected speech were thereby censored.[52]

---

[44] *Id.* at 246.

[45] *Id.* at 247-48.

[46] *Id.* at 253.

[47] *Id.*

[48] *Id.* at 254.

[49] *Id.*

[50] *Id.*

Concurring, Justice Thomas was more receptive to this "prosecution thwarting" argument than the majority. Thomas believed the government's fears here were speculative because it had not identified any cases of a defendant successfully raising such a defense, but he allowed that "technology may evolve to the point where it becomes impossible to enforce actual child pornography laws because the Government cannot prove that certain pornographic images are of real children."[53] Contrary to the majority's overbreadth point, Thomas reasoned that the government "may well have a compelling interest in barring or otherwise regulating some narrow category of 'lawful speech' in order to enforce effectively laws against pornography made through the abuse of real children."[54]

In partial concurrence, Justice O'Connor (joined by Chief Justice Rehnquist and Justice Scalia) also lent support to this rationale. With respect to images that are computer-generated and "virtually indistinguishable" from real images (i.e., "virtual child pornography"), O'Connor had real concern that "defendants indicted for the production, distribution, or possession of actual child pornography may evade liability by claiming that the images attributed to them are in fact computer-generated."[55] She worried that the "rapid pace of advances in computer-graphics technology" could soon make this danger real.[56] O'Connor would therefore have struck down the "appears to be" provision *only* as to "the subset of cases involving youthful adult pornography" (i.e., pornography involving adults who looked like minors).[57] Rehnquist and Scalia disagreed with her on that last point, finding limiting constructions of the provision as applied to "youthful adult pornography" that would make it applicable only to the "hard core of child pornography" already proscribable under *Ferber* (without explaining, however, how *Ferber* applies to "youthful-looking *adult* actors").[58]

---

[51] *Id.* at 255.

[52] *Id.*

[53] *Id.* at 259 (Thomas, J., concurring).

[54] *Id.* (Thomas, J., concurring).

[55] *Id.* at 263-64 (O'Connor, J., concurring).

[56] *Id.* at 264 (O'Connor, J., concurring).

The majority spent very little time in striking down the provision prohibiting material that was "advertised, promoted, presented, described, or distributed in such a manner that conveys the impression" it depicts "a minor engaging in sexually explicit conduct."[59] Focused not so much on the content of material as on how it is presented, this provision appeared to be a "pandering" provision.[60] While pandering may have some bearing on whether material is legally obscene, the CPPA provision went well beyond the parameters the Court had marked out in the past, and was therefore, the majority concluded, substantially overbroad.[61] For instance, the provision would have made all possessors of "pandered" material liable for prosecution, whether or not they themselves pandered the materials.

Responding to *Ashcroft*, in 2003 Congress passed the PROTECT Act, amending federal child pornography law. The definition of child pornography in § 2256(8)(B) (the "appears to be" provision invalidated by *Ashcroft*) was changed to "any visual depiction . . . where . . . such visual depiction is a digital image, computer image, or computer-generated image that is, or *is indistinguishable from*, that of a minor engaging in sexually explicit conduct."[62] The House Conference Report explains that

> [t]his section narrows the definition of child pornography under 18 U.S.C. § 2256(8)(B) to depictions that are "digital images" (e.g., picture or video taken with a digital camera),

---

[57] *Id.* at 266 (O'Connor, J., concurring).

[58] *Id.* at 269 (Rehnquist, C.J., concurring).

[59] *Id.* at 257-58; *see* 18 U.S.C. § 2256(8)(D) (2000) (repealed 2003).

[60] *See, e.g.*, Ginzburg v. United States, 383 U.S. 463 (1966).

[61] *Ashcroft*, 535 U.S. at 258.

[62] 18 U.S.C. § 2256(8)(B) (Supp. 2003) (emphasis added).

> "computer images" (e.g., pictures scanned into a computer), or "computer-generated images" (e.g., images created or altered with the use of a computer). The Supreme Court was concerned in [*Ashcroft*] that the breadth of the language would prohibit legitimate movies like *Traffic* or plays like *Romeo and Juliet.* Limiting the definition to digital, computer, or computer-generated images will help to exclude ordinary motion pictures from the coverage of "virtual child pornography."[63]

The House commentary further explains that the amended section

> further narrows the definition by replacing the phrase "appears to be" with the phrase "is indistinguishable from." That new phrase addresses the Court's concern that cartoon-sketches would be banned under the statute. "The substitution of 'is indistinguishable from' in lieu of 'appears to be' more precisely reflects what Congress intended to cover in the first instance, and eliminates an ambiguity that infected the current version of the definition and that enabled those challenging the statute to argue that it 'capture[d] even cartoon-sketches and statues of children that were sexually suggestive.'"[64]

Buttressing that line of thought, the amended law now defines "indistinguishable" as "virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct."[65] It also includes the caveat that "[t]his definition does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults."[66]

Furthermore, the definition of child pornography itself in § 2256(8)(B) (the revised "is, or indistinguishable from" provision) was narrowed by clarifying that any "simulated" sexually explicit conduct must be "lascivious," in addition to the other requirements of (8)(B) and (2)(B).[67] The House commentary explains that this narrowing of the definition of child pornography "require[s] a simulated image to be lascivious to constitute child pornography under the new definition in 18 U.S.C. § 2256(8)(B)," and therefore, "child pornography that simulates sexually explicit conduct must be lascivious as well as meet the other requirement of the definition."[68] Under the version struck down by *Ashcroft*, the combination of (2)(A) and (8)(B) would have permitted finding child pornography from a visual depiction that "appeared to be" of a minor engaging in "simulated" sexual intercourse, whether or not the simulated image was "lascivious." Additionally, "sexually explicit conduct" under (2)(B) was redefined, not only as "lascivious simulated sexual intercourse," but also as "*graphic* sexual intercourse."[69] Under the amended law, "graphic" means "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."[70] This is intended to clarify further the types of images proscribed as "virtual" child pornography under (8)(B). For reference purposes, the entirety of amended § 2256 appears below.[71]

---

[63] H.R. REP. NO. 108-66, at 60 (2003) (Conf. Rep.), *as reprinted in* 2003 U.S.C.C.A.N. 683, 695.

[64] *Id.*

[65] § 2256(11).

[66] *Id.*

---

[67] § 2256(2)(B).

[68] H.R. REP. NO. 108-66, at 60.

[69] § 2256(2)(B) (emphasis added).

[70] § 2256(10).

[71]

> (1) "minor" means any person under the age of eighteen years;
>
> (2)(A) Except as provided in subparagraph (B), "sexually explicit conduct" means actual or simulated—
>
> (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
>
> (ii) bestiality;
>
> (iii) masturbation;
>
> (iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the genitals or pubic area of any person;

(B) For purposes of subsection 8(B) of this section, "sexually explicit conduct" means—

(i) graphic sexual intercourse, including genital-genital, oral- genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(ii) graphic or lascivious simulated;

(I) bestiality;

(II) masturbation; or

(III) sadistic or masochistic abuse; or

(iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person;

(3) "producing" means producing, directing, manufacturing, issuing, publishing, or advertising;

(4) "organization" means a person other than an individual;

(5) "visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image;

(6) "computer" has the meaning given that term in section 1030 of this title;

(7) "custody or control" includes temporary supervision over or responsibility for a minor whether legally or illegally obtained;

(8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

[(D) Repealed. Pub.L. 108-21, Title V, § 502(a)(3), Apr. 30, 2003, 117 Stat. 678]

The 2003 amendments also include a "new and comprehensive" affirmative defense to distribution or possession of child pornography.[72] The amended law provides that subsections (1), (2), (3)(A), (4) and (5) of § 2252 are subject to the affirmative defenses that:

> (1)(A) the alleged child pornography was produced using an actual person or persons engaging in sexually explicit conduct; and (B) each such person was an adult at the time the material was produced; or
>
> (2) the alleged child pornography was not produced using any actual minor or minors.[73]

None of the affirmative defenses, however, are available for

> (9) "identifiable minor"—
>
> (A) means a person—
>
> (i)(I) who was a minor at the time the visual depiction was created, adapted, or modified; or
>
> (II) whose image as a minor was used in creating, adapting, or modifying the visual depiction; and
>
> (ii) who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and
>
> (B) shall not be construed to require proof of the actual identity of the identifiable minor.
>
> (10) "graphic", when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted; and
>
> (11) the term "indistinguishable" used with respect to a depiction, means virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct. This definition does not apply to depictions that are drawings, cartoons, sculptures, or paintings depicting minors or adults.

[72] *See* § 2252A(c).

[73] § 2252A(c)(1)-(2). The affirmative defenses are additionally subject to certain notice requirements.

offenses described under the so-called "morphing" provision.[74] The House commentary explains that the Court in *Ashcroft* seemed to leave open the possibility that a "more complete affirmative defense" provision could have contributed to saving the law's constitutionality.[75] In *Ashcroft*, the Court had read the previous affirmative defense provisions as affording defenses to distributors, but not possessors, of materials, and also as affording no affirmative defense to those who produce materials through computer imaging or other means that "do not involve the use of adult actors who appear to be minors."[76] The expanded affirmative defense provisions are designed to remedy those deficiencies.

A new pandering provision punishes any person who knowingly

> advertises, promotes, presents, distributes, or solicits through the mails, or in interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains—(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or (ii) a visual depiction of an actual minor engaging in sexually explicit conduct.[77]

The House Commentary explains that

> [t]his provision bans the offer to transact in unprotected material, coupled with proof of the offender's specific intent. Thus, for example, this provision prohibits an individual from offering to distribute anything that he specifically intends to cause a recipient to believe would be actual or obscene child pornography. It likewise prohibits an individual from soliciting what he believes to be actual or obscene child pornography. The provision makes clear that no actual materials need exist; the government establishes a violation with proof of the

---

[74] *See* § 2256(8)(C).

[75] H.R. REP. NO. 108-66, at 61 (2003) (Conf. Rep.), *as reprinted in* 2003 U.S.C.C.A.N. 683, 695.

[76] *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 255-56.

[77] § 2252A(a)(3)(B).

> communication and requisite specific intent. Indeed, even fraudulent offers to buy or sell unprotected child pornography help to sustain the illegal market for this material.[78]

This new pandering provision seems designed to remedy the overbreadth of the pandering provision struck down in *Ashcroft*.[79] As discussed below, however, this provision has already been invalidated by one federal circuit court as facially overbroad and vague.[80]

Finally, the amended law creates two new offenses related to child pornography but attacking the problem through different avenues. Section 2252A(a)(6) "creates a new offense that criminalizes the act of using any type of real or apparent child pornography to induce a child to commit a crime."[81] Section 1466A creates new offenses that target actual or simulated depictions of minors that meet the obscenity standards of *Miller*.[82] As the House Commentary explains, "[t]his section prohibits any obscene depictions of minors engaged in any form of sexually explicit conduct and prohibits a narrow category of 'hardcore' pornography involving real or apparent minors, where such depictions lack literary, artistic, political, or scientific value."[83]

III. SELECTED ISSUES ADDRESSED BY LOWER COURTS

A. *The Limits of* Ashcroft

Several federal circuit courts have reached the seemingly obvious conclusion that *Ashcroft* was strictly limited to overruling the "appears to be" provision of previous § 2256(8)(B) and the expanded "pandering" provision of previous § 2256(8)(D). Consequently, the decision did not touch other provisions in § 2256 or other federal child pornography laws.[84] In a similar vein, federal courts have concluded that a conviction under § 2422(b) (attempting to "coerce and entice" a minor to engage in sexual activity) is not called into question by *Ashcroft*, where a government agent posed as a minor in an internet chat room.[85] Thus, notwithstanding *Ashcroft*, an actual minor is not constitutionally necessary for an attempt conviction under § 2242(b).

---

[78] H.R. REP. NO. 108-66, at 61-62.

[79] *See supra* note 62 and accompanying text; *see also* 18 U.S.C. § 2256(8)(D) (repealed 2003).

[80] *See infra* Part III.D.

[81] H.R. REP. NO. 108-66, at 62.

[82] *See id.*

[83] *Id.* The commentary goes on to explain that the offense in § 1466A is "subject to the penalties applicable to child pornography, not the lower penalties that apply to obscenity, and it also contains a directive to the U.S. Sentencing Commission requiring the Commission to ensure that the U.S. Sentencing Guidelines are consistent with this fact." *Id.*

In *United States v. Bach*, the Eighth Circuit upheld a conviction under § 2256(8)(C) (the "morphing" provision) where a nude, sexually explicit photo of a 16-year-old boy had been altered to have the face of the actual boy replaced by the face of a "well-known child entertainer." The image still fell within *Ferber* because it involved the image of an actual minor.[86] The *Bach* court seemed to focus on the harm to the "child entertainer" from having the altered image distributed, as opposed to the harm to the unidentified minor from making the photo to begin with. Finally, *Bach* left open the possibility that certain applications of § 2256(8)(C) might be unconstitutional under *Ashcroft,* without specifying what kind of applications.[87]

The *Bach* court also addressed, and rejected, the argument that the right to privacy recognized by the Supreme Court in *Lawrence v. Texas* calls into question this particular conviction under federal child pornography laws.[88] In *Bach*, a 40-year-old man took and transmitted pictures of a 16-year-old boy masturbating and engaging in oral sex (apparently different photos than the one at issue in the "morphing" discussion, *supra*).[89] Notably, in this case, the relevant state age of consent (Minnesota) was 16, whereas federal law defined "minor" as under 18. The court reasoned that the federal government's definition of "minor" as "under 18" was rationally related to its interest in enforcing child pornography laws, notwithstanding the divergence from the Minnesota age of consent.[90]

---

[84] *See, e.g.*, United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003); *accord* United States v. Deaton, 328 F.3d 454 (8th Cir. 2003); United States v. Kelly, 314 F.3d 908, 911 (7th Cir. 2003); United States v. Richardson, 304 F.3d 1061, 1063-64 (11th Cir. 2002).

[85] United States v. Davis, 2006 WL 226038 (10th Cir. 2006), *cert. denied*, 126 S. Ct. 2918 (2006); *accord* United States v. Thomas, 410 F.3d 1235 (10th Cir. 2005); United States v. Meek, 366 F.3d 705 (9th Cir. 2004); United States v. Root, 296 F.3d 1222 (11th Cir. 2002).

[86] United States v. Bach, 400 F.3d 622 (8th Cir. 2005), cert. denied, 126 S. Ct. 243 (2005).

[87] *See id.* at 631-32.

[88] *See id.* at 628-29; *see also* Lawrence v. Texas, 539 U.S. 558 (2003).

B. Ashcroft *and Evidentiary Standards*

Several federal courts have concluded that *Ashcroft* did not establish a categorical rule of evidence requiring expert testimony to prove that an unlawful image is of a real child. In many cases, juries can distinguish between real and virtual images.[91] Under federal child pornography laws, however, the government does bear the burden of proving that children depicted in allegedly unlawful images are real children.[92] Thus, the First Circuit found that the defendant had a right to have a fact-finder (in this case, the trial court) decide whether the depicted children were real.[93] Reversing the conviction, the First Circuit found this was *not* done, even where the trial court had accepted expert testimony that the images satisfied the "Tanner Scale" (which categorizes the physical characteristics of children).[94] The court reasoned that the Tanner Scale findings would have also been consistent with youthful-looking adults.[95] Consistent with this, however, other courts have concluded that the government need not necessarily produce evidence *in addition to* the computer images to prove that real children are depicted in the computer images.[96] The Illinois Supreme Court's reasoning in *People v. Normand* is illustrative:

---

[89] *Id.* at 622.

[90] *See id.* at 629.

[91] United States v. Kimler, 335 F.3d 1132 (10th Cir. 2003); *accord* United States v. Irving, 432 F.3d 401 (2d Cir. 2005), *withdrawn & superseded on reh'g*, 432 F.3d 401 (2d Cir. 2006); United States v. Deaton, 328 F.3d 454 (8th Cir. 2003); United States v. Hall, 312 F.3d 1250 (11th Cir. 2003).

[92] *See, e.g.*, United States. v. Hilton, 386 F.3d 13 (1st Cir. 2004).

[93] *Id.* at 18-19.

[94] *Id.*

[95] *Id.*

> If child pornographers had easy access to the technology to produce virtual child images that are indistinguishable from images using real children, no reason would exist to use real children. The risk of prosecution and prison sentences for using real children contrasts sharply with the legality of using virtual child images. Few pornographers would be willing to take that risk if a legal means of producing the same type of images existed. Yet, if virtual child pornography exists, it has not been well publicized. Given the substantial market for child pornography on the Internet, it stands to reason that such a radical development would not go unnoticed, especially in legal and law enforcement circles. Therefore, we are not convinced that this technology is so widely available that the State must be required as a matter of law to produce evidence in addition to the images themselves to carry its burden of proof.[97]

C. "Unit of Prosecution" in Child Pornography Cases

A few courts have addressed the difficult issue of the appropriate "unit of prosecution" in child pornography cases—that is, whether counts against defendants should be grouped by individual images, by websites, or by some other grouping. In *United States v. Reedy*, the Fifth Circuit decided that, given the ambiguity of § 2252 on this question, the "rule of lenity" required that counts against a defendant be grouped by website, as opposed to individual image.[98] Recently, in a case of apparent first impression, *State v. Kujawa*, the Louisiana First Circuit Court of Appeals approved the imposition, under state law, of fifteen counts of child porn possession for fifteen separate images.[99] The *Kujawa* court reasoned that the question was essentially one of statutory construction, concluding that "[a] careful reading of the entire statute reveals that the legislative intent was to proscribe possession of any single image. The use of the plural form was clearly a matter of grammatical style and not suggestive of an intent to establish a unit of prosecution based upon a broad course of conduct involving multiple contraband images."[100] The relevant Louisiana law defined child pornography as "[t]he photographing, videotaping, filming, or otherwise reproducing visually of any sexual performance involving a child under the age of seventeen," and in turn defined "sexual performance" as "any performance or part thereof that includes sexual conduct involving a child under the age of seventeen."[101]

---

[96] *See* People v. Normand, 831 N.E.2d 587 (Ill. 2005); *accord* United States v. Slanina, 359 F.3d 356 (5th Cir.), *cert. denied*, 543 U.S. 845 (2004); *Kimler*, 335 F.3d 1132; *Hall*, 312 F.3d 1250.

[97] *Normand*, 831 N.E.2d at 595.

[98] 304 F.3d 358 (5th Cir. 2002).

D. Review of the 2003 Amendments

No federal or state appellate decisions have yet addressed the constitutionality of the new "indistinguishable from" provision in § 2256(8)(B).[102] One is thus left to speculate whether the change from "appears to be" to "indistinguishable from" will really make a difference to the amended law's adherence to First Amendment standards. Congress seems to be betting on the strength of the "prosecution thwarting" rationale of Justices like Thomas and O'Connor (who partially concurred in *Ashcroft*). But the five-justice majority that rather forcefully repudiated that rationale is still on the Court. The replacement of Chief Justice Rehnquist by John Roberts, and Justice O'Connor by Samuel Alito, does not disturb that balance. While doctrinal alteration is certainly possible in this area, it seems unlikely that the "indistinguishable from" provision will be upheld under *Ashcroft*.

---

[99] State v. Kujawa, 929 So.2d 99 (La. Ct. App. 2006). *Kujawa* has a good general discussion of the unit of prosecution issue, referencing *Reedy*, as well as decisions in United States v. Esch, 832 F.2d 531 (10th Cir. 1987); Vineyard v. State, 958 S.W.2d 834 (Tex. Crim. App. 1998) (en banc); State v. Mather, 646 N.W.2d 605 (Neb. 2002); State v. Multaler, 643 N.W.2d 437 (Wis. 2002); State v. Schaefer, 668 N.W.2d 760 (Wis. Ct. App. 2003); Commonwealth v. Davidson, 860 A.2d 575 (Pa. Super. Ct. 2004); and State v. Howell, 609 S.E.2d 417 (N.C. Ct. App. 2005).

[100] *Kujawa*, 929 So.2d at 111 .

[101] La. Rev. Stat. Ann. § 14:81.1(A)(1), (B)(1) (2006).

[102] *See supra* notes 62, 64-66 and accompanying text.

One federal circuit court has recently addressed the amended pandering provision in § 2252A(a)(3)(B), which was intended to remedy the pandering provision struck down by *Ashcroft*.[103] In a thorough opinion, the Eleventh Circuit in *United States v. Williams* said essentially that Congress had provided a partial and inadequate fix to the former provision's defects. *Williams* struck down the new pandering provision as both unconstitutionally overbroad and vague.[104] William's possession of child pornography under § 2252A(a)(5)(B) was upheld, but an additional pandering conviction was overturned. In an internet chat room, Williams had told an undercover federal agent that he had sexually explicit photos of his own four-year-old daughter. A subsequent search of Williams' computer revealed at least twenty-two images of actual child pornography. Williams was convicted, not only of possession of child pornography, but also with "promoting . . . material 'in a manner that reflects the belief, or that is intended to cause another to believe,' that the material contains illegal child pornography."[105]

The court provided a detailed and helpful summary both of the problem of child pornography and of Congress's efforts to combat it. The court was refreshingly candid about how the online world exacerbates the problem of stamping out the disease:

> The anonymity and availability of the online world draws those who view children in sexually deviant ways to websites and chat rooms where they may communicate and exchange images with other like-minded individuals. The result has been the development of a dangerous cottage industry for the production of child pornography as well as the accretion of

---

[103] *See supra* note 40 and accompanying text.

[104] United States v. Williams, 444 F.3d 1286 (11th Cir. 2006).

[105] *Id.* at 1288-89; *see also* 18 U.S.C. § 2252A(a)(3)(B) (Supp. 2003).

> ever-widening child pornography distribution rings. Our concern is not confined to the immediate abuse of the children depicted in these images, but is also to enlargement of the market and the universe of this deviant conduct that, in turn, results in more exploitation and abuse of children. Regulation is made difficult, not only by the vast and sheltering landscape of cyberspace, but also by the fact that mainstream and otherwise innocuous images of children are viewed and traded by pedophiles as sexually stimulating.[106]

Unhappily for the government's case, however, the court was equally clear-eyed about the limits on its efforts imposed by the First Amendment and the Supreme Court's approach in *Ashcroft*.

The *Williams* court did recognize that the amended pandering provision had cleared up some of the prior law's defects. The law no longer criminalized pandered materials "for all purposes in the hands of any possessor based on how they were originally pandered."[107] Instead, the focus now shifted from "regulation of the underlying material to regulation of the speech related to the material."[108] Furthermore, Congress had evidently abandoned the "secondary effects and market deterrence justifications" disapproved in *Ashcroft*, in favor of a renewed emphasis on the "prosecution thwarting" problem posed by computer generated child porn.[109] But these improvements to the law were insufficient to overcome the problems of overbreadth and vagueness.

The court focused on the amended provision's de-coupling of pandering words from the nature of the material pandered. No actual or even simulated child pornography need exist, since the provision embraces "purported" material. According to the court, this means that pandering speech is "criminalized even when the touted materials are clean or non-existent."[110]

---

[106] *Williams*, 444 F.3d at 1290 (footnote omitted).

[107] *Id.* at 1295.

[108] *Id.*

[109] *Id.*

[110] *Id.* at 1298. The court explained that "any promoter—be they a braggart, exaggerator, or outright liar—who claims to have illegal child pornography mate-

Essentially, since there was no requirement of any illegal or potentially illegal materials associated with the pandering, the amended provision would criminalize speech amounting to the advocacy of *future* illegal conduct. The law, of course, may not constitutionally forbid even speech advocating illegal conduct unless it rises to the level of *Brandenburg*-type incitement or other unprotected categories.[111] Furthermore, the law's criminalization of speech that merely "reflects the belief" that material is real or simulated child porn—when the material may not actually be anything of the kind—raises the specter that the law could penalize the "deluded" pandering of innocuous materials or, worse, "the thoughts conjured up by . . . legal materials."[112] The court simply rejected additional congressional findings that the pandering provision was necessary to drying up the market for child porn, observing that "Congress has again failed to articulate specifically how the pandering and solicitation of legal images, even if they are promoted or believed to be otherwise, fuels the market for illegal images of real children engaging in sexually explicit conduct."[113] Finally, the court also found that the "purported" and "reflects the belief" aspects of the amended provision were unconstitutionally vague, "fail[ing] to convey the contours of its restriction with sufficient clarity to permit law-abiding persons to conform to its requirements."[114]

---

rials is a criminal punishable by up to twenty years in prison, even if what he or she actually has is a video of 'Our Gang,' a dirty handkerchief, or an empty pocket." *Id.*

[111] *Id.*; *see supra* notes 7-9 and accompanying text.

[112] *Williams*, 444 F.3d at 1299-1300. The court also found inapposite the government's attempt to categorize the amended provision as the kind of pandering law approved by the Supreme Court in *Ginzburg v. United States*: that case had merely allowed evidence of pandering as probative of the *Miller* obscenity standard. *Id.* at 1300-1302; *see* Ginzburg v.United States, 383 U.S. 463 (1966). The court also suggested that *Ginzburg* may also no longer be good law after the Supreme Court's decision in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, that afforded commercial speech greater First Amendment protection. *See* 425 U.S. 748 (1976); *Williams*, 444 U.S. at 1301-02.

[113] *Williams*, 444 F.3d at 1303-04.

[114] *Id.* at 1305-07.

SHOULD ONLINE DEFAMATION BE CRIMINALIZED?

Susan W. Brenner[*]

I. INTRODUCTION

"'People's reputations are sullied in a very new way, and it's very hard for them to recover from that.'"[1]

As Part III of this article explains, the continuing evolution of the Internet fundamentally alters the assumptions that shaped our approach to criminal defamation.[2] Like most of our law, our approach to criminal defamation derives from historical English common law; as Part II explains, English courts "invented" four libel offenses in the sixteenth century as part of an effort to control the misuse of a then new technology, the printing press.

Colonists brought these offenses to America, where they ultimately languished, leading the drafters of the Model Penal Code to recommend that defamation *not* be criminalized.[3] That recommendation, coupled with Supreme Court decisions applying the First Amendment to libel laws, caused criminal defamation to fall into disrepute and decline in this country.[4]

This article analyzes whether we should reconsider criminalizing defamation given the ever-increasing influence of the Internet. Some contend that criminal defamation is the only realistic option we have for controlling certain types of online defamation. Those who take this view point out that the drafters of the Model Penal Code issued their recommendation in 1961, when publication was limited to print and instruments of the mainstream media (MSM).[5] They note that these instruments were all controlled by corporate actors whose business acumen reduced the likelihood that defamatory material would be published and whose deep pockets made civil liability a viable option for the victim if this did, in fact, occur.[6] Those who argue for expanding our use of criminal defamation point out that computer technology has, in effect, leveled the playing field; today, anyone with access to the Internet can publish whatever he or she likes, however inaccurate and/or scurrilous it may be.[7]

---

[*] NCR Distinguished Professor of Law & Technology, University of Dayton School of Law.

[1] Lisa Sink & Linda Spice, *Man Charged with Defamation: Disgruntled Fired Employee Accused of Posting Ad with Ex-boss' Name on Internet*, MILWAUKEE J. SENTINEL, June 7, 2000, at B1 (quoting state representative Marlin Schneider) (emphasis added).

[2] *See infra* Part II.A for the definition of defamation.

[3] *See infra* Part II.C.

[4] *See infra* Part II.C, II.D.

Those who advocate resuscitating criminal defamation contend that cyberspace vastly expands the incidence and virulence of published defamatory speech.[8] They also argue that since most of these online publishers are judgment-proof individuals, civil liability can neither make their victims whole nor deter those who may be inclined to follow their lead.[9]

Criminalizing speech is generally distasteful to Americans because of our deep reverence for the First Amendment; we tend to believe an uninhibited marketplace of ideas is one of the best guarantees of freedom.[10] Freedom, however, is not inherently inconsistent with restrictions; every society necessarily outlaws behaviors that "harm" others and, in so doing, threaten the elemental fabric of social order.[11] It is therefore conceptually appropriate to explore the possibility that our ever-increasing access to cyberspace may warrant rethinking how we use legal rules to deter harmful speech. We return to that issue in Part IV. First, we need to review how we have arrived at the current state of affairs, in which criminal liability is rarely imposed on those whose speech defames others.

---

[5] *See infra* Part III.A, III.C. We will use the omnibus term mainstream media (MSM) to denote media venues that once represented the *only* outlets for publication and are still influential in this area. *See generally* Noam Chomsky, *What Makes Mainstream Media Mainstream*, Z Magazine, Oct. 1997, *available at* http://www.chomsky.info/articles/199710—.htm; Wikipedia, *Mainstream Media*, http://en.wikipedia.org/wiki/Media (last visited Jan. 14, 2007); *see also* Robert McChesney, *The Global Media Giants: We Are the World*, EXTRA!, Nov./Dec. 1997, *available at* http://www.fair.org/index.php?page=1406.

[6] *See infra* Part IV; *see infra* Part II.A for the definition of publication and publish.

[7] *See infra* Part IV; *see, e.g.*, Barrick Gold Corp. v. Lopehandia, [2004] 71 O.R.3d 416 (Can).

[8] *See infra* Parts III, IV.

[9] *See infra* Parts III, IV.

[10] *See, e.g.*, McConnell v. FEC, 540 U.S. 93, 265 (2003) (Thomas, J., dissent-

II. CRIMINAL DEFAMATION IN ANGLO-AMERICAN LAW

> *"All four branches of libel sought to ensure that speech did not violate established norms of respect and propriety."*[12]

This section defines essential terms and traces the evolution of criminal defamation law from its emergence in sixteenth century England to its current, rather neglected state in modern American law. The goal is to provide a doctrinal foundation for the analysis presented in Part IV.

A. Definitions

The first term we need to define is defamation. Historically, the justification for criminalizing defamation was to deter the publication of communications that were likely to cause a breach of the peace, specifically, a duel or some other form of self-help.[13] As with all criminal prohibitions, therefore, the

---

ing) ("The very 'purpose of the First Amendment [is] to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail.'" (quoting Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969)) (alteration in original).

[11] *See, e.g.*, Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, 10 B.U.J. SCI. & TECH. L. 1, 6-46 (2004).

[12] Robert C. Post, *Cultural Heterogeneity and Law: Pornography, Blasphemy, and the First Amendment*, 76 CAL. L. REV. 297, 305 (1988) (emphasis added). For the four branches of common law libel, see *infra* Part II.B.

[13] *See, e.g.*, Garrison v. Louisiana, 379 U.S. 64, 68 (1964). "Although the victim of a . . . defamatory publication might not have been unjustly damaged in reputation by the libel, the speaker was still punishable since the remedy was

goal was to deter speech that threatened the social order.[14] The justifications for imposing civil liability have always focused more on injury to the individual. The *Restatement of Torts*, for example, defines a defamatory communication as one that "tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[15]

This civil concern with individual harm influenced the evolution of criminal libel law in nineteenth and early twentieth century America, so that it, too, came to focus on the injury a communication inflicted upon "the person defamed, regardless of its effect upon the public."[16] As a result, while some modern criminal libel laws target only public harm,[17] *i.e.*, the potential for causing a breach of the peace, others target communications that "blacken the memory" of the deceased or "impeach the . . . integrity, virtue, or reputation or expose the natural defects of one who is alive and thereby . . . expose him to public hatred, contempt, or ridicule."[18]

---

designed to avert the possibility that the utterance would provoke an enraged victim to a breach of peace." *Id. See also* Beauharnais v. Illinois, 343 U.S. 250, 254 (1952); 50 AM. JUR. 2D *Libel and Slander* § 523 (2005).

[14] *See* Brenner, *Toward A Criminal Law for Cyberspace*, *supra* note 11, at 6-46.

[15] RESTATEMENT (SECOND) OF TORTS § 559 (1977).

[16] 50 AM. JUR. 2D *Libel and Slander* § 523 (2005) (citing Garrison v. Louisiana, 379 U.S. 64 (1964); Ashton v. Kentucky, 405 S.W.2d 562 (Ky. 1965), *rev'd on other grounds*, 384 U.S. 195 (1966)). "Thus, under the rule prevailing in various jurisdictions, criminal liability may be incurred by the publication of a statement which tends to expose a living person to such matters as hatred, contempt, disgrace, ridicule, or loss of confidence." *Id.* (citing Krasner v. Alabama, 26 So. 2d 519 (Ala. Ct. App. 1946), *rev'd on other grounds*, 26 So. 2d 526 (Ala. 1946); Allen v. Texas, 189 S.W.2d 753 (Tex. Crim. App. 1945)).

[17] *See, e.g.*, ALA. CODE § 13A-11-160 (2006); GA. CODE ANN. § 16-11-40 (2003); N.H. REV. STAT. ANN. § 644:11 (2002); S.C. CODE ANN. § 16-7-150 (2003); VA. CODE ANN. § 18.2-417 (2004).

[18] COLO. REV. STAT. § 18-13-105 (2006); *see, e.g.*, IDAHO CODE ANN. § 18-4801 (2004); KAN. STAT. ANN. § 21-4004 (1995); LA. REV. STAT. ANN. § 14:47 (1997); MINN. STAT. § 609.765 (2006); MONT. CODE AN. § 45-8-212 (2004); N.M. STAT. ANN. § 30-11-1 (2004); N.D. CENT. CODE § 12.1-1501 (1997); OKLA. STAT. ANN. tit. 21, § 771 (West 2002); UTAH CODE ANN. § 76-9-501 (2003); WASH. REV. CODE ANN. § 9.58.010 (West 2003); WIS. STAT. ANN. § 942.01 (West 2006); *see also* 50 AM. JUR. 2D *Libel and Slander* § 532 (2005).

Tort law divides defamation into libel and slander.[19] Libel consists of publishing defamatory material in written and/or printed form, while slander consists of publishing such material by spoken words or gestures.[20] A very few states separately criminalize libel and slander,[21] but most follow traditional English common law and apply the generic term libel to *any* publication of defamatory material.[22]

The last two terms we need to define are publication and publish. *Black's Law Dictionary* defines publication as communicating defamatory material "to someone other than the person defamed;"[23] *Black's* also includes this element in its definition of publish.[24] The requirement that the material have been communicated to someone *other* than the person being defamed derives from the justifications for imposing civil liability on libelers and slanderers; as tort law "protects only the interest in reputation. Therefore, unless the defamatory matter is communicated to a third person there has been no loss of reputation . . . ."[25] This requirement has not been a component of criminal defamation law, presumably because its concern was with preventing breaches of the peace instead of protecting reputation; the offense of criminal libel is therefore committed as long as the defamatory material has been published to *anyone* other than its author or publisher.[26]

---

[19] *See, e.g.*, 50 AM. JUR. 2D *Libel and Slander* § 1 (2005).

[20] *See* RESTATEMENT (SECOND) OF TORTS § 568 (1977). For the historical origins of this distinction, see, for example, RESTATEMENT (SECOND) OF TORTS § 568 cmt. b (1977).

[21] *See, e.g.*, OKLA. STAT. ANN. tit. 21 § 781 (West 2002); UTAH CODE ANN. § 76-9-507 (2003); *see also* 53 C.J.S. *Libel & Slander* § 16 (2005) "While slander [was] not a crime at common law, it is a criminal offense under some . . . statutory provisions." *Id.* (footnote omitted) (citing New Jersey v. Klapprott, 22 A.2d 877 (N.J. 1941); California v. Faber, 77 P.2d 921 (Cal. App. Dep't Super. Ct. 1938); Branigan v. Wisconsin, 244 N.W. 767 (Wis. 1932)).

[22] For the evolution of English criminal libel law, see *infra* Part II.B.

[23] BLACK'S LAW DICTIONARY 1264-65 (8th ed. 2004); *see* RESTATEMENT (SECOND) OF TORTS § 577 (1977).

[24] BLACK'S LAW DICTIONARY 1268-69 (8th ed. 2004).

[25] RESTATEMENT (SECOND) OF TORTS § 577 cmt. b (1977). At lease one state has incorporated this requirement into its criminal defamation law, apparently in an effort to maintain consistency between civil and criminal defamation law. *See, e.g.*, LA. REV. STAT. ANN. § 14:47 (1997).

As noted earlier, civil law divides defamation into two categories based on the means used to communicate the defamatory material. Libel results when the material is communicated in written form, while slander consists of communicating it orally or by gesture. As was also noted earlier, criminal defamation law has generally resisted this categorization. Criminal defamation law has not, however, completely resisted a concern with *how* defamatory material is communicated. A few states, at least, amended their criminal defamation statutes to ensure that they encompass publication by electronic and other technological means.[27]

B. History

As Part I noted, societies must control certain behaviors to maintain the baseline of social order that is essential for the existence and functioning of any society.[28] For most of our history, societies were concerned only with controlling physical behaviors; societies were not particularly concerned about controlling speech as long as it was oral, since face-to-face communication is limited in scale and it is relatively easy to correlate spoken words with a speaker.[29]

The rise of written language produced some concern about controlling speech because a speaker can use script to transcend the geographical limitations and attribute risks that are inherent in face-to-face oral communication.[30] A dissident can transcribe a diatribe and send it to a geographically dispersed audience, each of whom reads it and passes it on.[31] The use of script can also let the author conceal his identity and thereby frustrate official efforts to hold him accountable for what he has said.[32] Generally, though, script did not create significant control issues for those who wished to see that speech stayed within what they considered acceptable bounds.[33] Scale was still a problem; each copy of a diatribe had to be individually transcribed, which was a time-consuming process.[34] And it was relatively easy to identify speakers given that (i) only a small proportion of the populace was literate and (ii) handwriting is distinctive.[35]

---

[26] *See* 50 AM. JUR. 2D *Libel and Slander* § 525 (2005); *see, e.g.*, McCurdy v. Hughes, 248 N.W. 512, 517-518 (N.D. 1933); *see also* Gregory C. Lisby, *No Place in the Law: The Ignominy of Criminal Libel in American Jurisprudence*, 9 COMM. L. & POL'Y 433, 440 (2004); *cf.* MONT. CODE ANN. § 45-8-212(2) (2004).

[27] *See, e.g.*, MONT. CODE ANN. § 45-8-212(2) (2004) (electronic); WASH. REV. CODE ANN. § 9.58.010 (West 2003) (radio).

[28] *See supra* note 11 and accompanying text.

[29] *See* Susan W. Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data Be Criminalized*, 13 ALB. L.J. SCI. & TECH. 273, 280-84 (2003).

[30] *See id.*

This changed with the development of the first communication technology: the printing press. With a press, one can produce hundreds or thousands of copies of a diatribe quickly and anonymously. The copies can then be distributed over as wide a geographical area as physical transport allows, and they can be distributed simultaneously, rather than sequentially.[36] It did not take governments long to realize that printing threatened their ability to control speech. The first printing press was brought to England in 1476; by 1538, a royal proclamation required that one obtain a license from the Privy Council before printing a book.[37] This licensing system ended in 1694, and the common law courts became responsible for controlling speech, written and oral; they developed the concept of criminal libel and used it for this purpose.[38]

Common law criminal libel actually encompassed four distinct offenses: seditious libel; blasphemy; obscenity; and defamation.[39] Seditious libel consisted of publishing material that defamed the government and/or its officials; blasphemy consisted of publishing material that "reviled" God or religion; obscenity consisted of publishing "offensive sexual content;" and defamation (which came to be known simply as criminal libel) consisted of publishing material that defamed a private citizen.[40] The colonists who left England brought all four offenses with them to the New World, where they have had rather different histories.[41]

---

[31] *See id.*

[32] *See id.*

[33] *See id.*

[34] *See id.*

[35] *See id.*

[36] *See id.*

[37] *See id.*

[38] *See id.*

[39] *See id.* at 288.

English authorities took seditious libel very seriously, and their efforts to enforce it in the American colonies were a source of tension between the colonists and British authorities.[42] Since the Revolution, seditious libel has cropped up on occasion in federal law, but it has never become a stable component of American law because its prohibitions are inconsistent with the free speech guarantees of the First Amendment.[43] As to blasphemy, English authorities seem not to have been terribly concerned about publications that reviled God,[44] but Puritan colonists certainly were.[45] Other colonists, however, were not, and the adoption of the First Amendment guaranteed that blasphemy would not be a component of American criminal law.[46] Obscenity was never a priority in English law; although the principle that publishing obscene material was a criminal act was established by 1727, English courts did not define obscenity until 1868.[47] The Puritans and other English colonists consequently did not bring a fully-realized concept of the offense with them when they came to the New World; as a result, perhaps, prosecuting obscenity did not become a priority in America until the end of the nineteenth century, when a group of "bluestockings" successfully lobbied for the criminalization of prurient material.[48] By the end of the twentieth century, however, obscenity prosecutions were rare, their decline a product of evolving community standards.[49]

---

[40] *See id.* at 290-316.

[41] *See id.*

[42] *See id.* at 290-92; *see also* David A. Anderson, *The Origins of the Press Clause*, 30 UCLA L. REV. 455, 509-14 (1983).

[43] *See* Brenner, *Complicit Publication*, *supra* note 29, at 304-05.

[44] *See id.* at 290-316.

[45] Blasphemy was a capital crime in the Massachusetts Bay Colony. *See, e.g.*, Linda L. Ammons, *What's God Got to Do With It? Church and State Collaboration in the Subordination of Women and Domestic Violence*, 51 RUTGERS L. REV. 1207, 1245-46 (1999).

[46] *See* Brenner, *Complicit Publication*, *supra* note 29, at 305-07.

[47] *See id.* at 307-08.

Though all four of the English offenses technically constituted criminal libel, we are only concerned with the fourth offense, which was variously known as defamation or criminal libel. As noted earlier, English law recognized a distinction between seditious libel and criminal libel:

> In 1605, . . . the Court of Star Chamber used the Roman doctrine of *libellis famosus* to criminalize libel directed toward an individual. The Court's rationale for criminalizing non-seditious defamation was that libels . . . may be penalized . . . because they tend to create breaches of the peace when the defamed . . . undertake to revenge themselves on the defamer. As one scholar explained, ". . . the great vogue of . . . dueling . . . seems to have given cause for great concern to the government." After 1605, . . . when defamation involved a public official, it "was considered . . . a threat to the security of the state" and prosecuted as seditious libel; when it involved a private person, "it was considered to risk a breach of the peace" and . . . prosecuted as criminal libel.[50]

English colonists brought this approach to individual criminal defamation to the New World, where defamation of public officials was eventually subsumed into criminal libel; seditious libel, insofar as it continued to exist, was reserved for attacks on the government.[51]

Since the common law approached criminal libel as a threat to the social order (rather than as the infliction of harm on an individual), it was enforced more stringently than was its civil counterpart: Truth was a defense in civil libel actions, but not in prosecutions for criminal libel.[52] The colonists brought this distinction with them to this country, where it was influential well into the twentieth century.[53]

---

[48] *See id.* at 308-15.

[49] *See id.*; *see, e.g.*, Stanley v. Georgia, 394 U.S. 557, 564-65 (1969).

[50] Brenner, *Complicit Publication*, *supra* note 29, at 316 (ninth alteration in original) (footnotes omitted) (quoting THEODORE F.T. PLUCKNETT, A CONCISE HISTORY OF THE COMMON LAW 490 (5th ed. 1956); Lisa K. West, Note, Milkovich v. Lorain Journal Co.—*Demise of the Opinion Privilege in Defamation*, 36 VILL. L. REV. 647, 654 (1999)).

[51] *See, e.g.*, Lisby, *supra* note 26, at 464.

C. Defamation in America

The conception of criminal libel English colonists brought to this country has rarely been used. A quantitative study of criminal libel prosecutions in the colonies and, later, in the United States found no reported cases for the period 1658-1796.[54] The total number of reported cases for the seven decades spanning 1797 to 1877 never exceeded fifteen per decade, and tended to be in the single digits.[55] The number of reported cases increased to sixty in the 1877-1886 era and rose again, into the nineties, where it stayed for the period 1887-1916.[56] The total number of reported criminal libel prosecutions then began a decline, falling into the fifties for the period 1917-1936.[57] It continued its decline, hovering around twenty for the four decades between 1937 and 1976.[58] The next two decades saw a further decline in reported criminal libel prosecutions, falling to ten for 1977-1986 and five for 1987-1996.[59] The authors of the study found only two reported criminal libel cases for the period between 1997 and 2002, when the study ended.[60]

---

[52] *See supra* note 14 and accompanying text; *see, e.g.*, Marc A. Franklin, *The Origins and Constitutionality of Limitations on Truth as a Defense in Tort Law*, 16 STAN. L. REV. 789, 791-92 (1964). Indeed, a common law maxim held that "'the greater the truth, the greater the libel.'" State v. Browne, 206 A.2d 591, 595 (N.J. Super. Ct. App. Div. 1965) (quoting John Kelly, *Criminal Libel and Free Speech*, 6 U. KAN. L. REV. 295, 302 (1958)).

[53] *See, e.g.*, Edward L. Carter, *Outlaw Speech on the Internet: Examining the Link Between Unique Characteristics of Online Media and Criminal Libel Prosecutions*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 289, 295 (2005).

[54] *See* Lisby, *supra* note 26, at 467.

[55] *See id.* at 466. The precise numbers are as follows: 1797-1806 (seven); 1807-1816 (seven); 1817-1826 (eight); 1827-1836 (eleven); 1837-1846 (fourteen); 1847-1856 (fourteen); 1857-1866 (one); and 1867-1876 (fifteen). *Id.*

[56] *See id.* The precise numbers are 1887-1896 (ninety-nine); 1897-1906 (ninety-eight); and 1907-1916 (ninety-three). *Id.*

[57] *See id.* The precise numbers are 1917-1926 (fifty-two) and 1927-1936 (fifty). *Id.*

[58] *See id.* The precise numbers are 1937-1946 (twenty); 1947-1956 (nineteen); 1957-1966 (nineteen); and 1967-1976 (nineteen). *Id.*

The drafters of the Model Penal Code cited this sparsity of libel prosecutions as a factor that militated against using penal sanctions to control "personal calumny."[61] They said "[o]ne of the hardest questions" they confronted in drafting the Model Penal Code was deciding "whether to penalize anything like libel."[62] The architects of the Code began their analysis of this issue by explaining that "penal sanctions cannot be justified merely by the fact that defamation is . . . damaging to a person in ways that entitle him to maintain a civil suit."[63] After noting that "we reserve the criminal law for harmful behavior which exceptionally disturbs the community's sense of security," they considered whether libel falls into this category.[64]

They explained that behavior exceptionally disturbs the community's sense of security for either of two reasons: One is that the

> [H]arm done is very grave, as in rape or murder, so that even the remote possibility of being similarly victimized terrifies us. Or our alarm may, as in the case of petty theft or malicious mischief, derive from the higher likelihood that such lesser harms will be inflicted upon us by those who manifest disregard of other people's ownership.[65]

The drafters of the Model Penal Code concluded that "personal calumny falls in neither of these classes in the U.S.A., that it is therefore inappropriate for penal control, and that this probably accounts for the paucity of prosecutions and the near desuetude of . . . criminal libel legislation in this country."[66] They therefore chose not to include a criminal libel provision in the final version of the Model Penal Code, which appeared in 1962.[67]

---

[59] *See id.*

[60] *See id.* at 467. Analysis of the cases showed that a significant percentage of them involved the alleged defamation of public officials. *See id.* The percentages vary from 37.65% for all of the reported cases to 52.17% for the period between 1990 and 2002. *See id.*

[61] Model Penal Code § 250.7 cmt. at 44 (Tentative Draft No. 13, 1961).

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

The architects of the Code noted, though, that while "penal law need not address itself to . . . irritating or malicious gossip, or to the ordinary case of defamation compensable in a civil suit, it may very well have to take cognizance of certain aggravated situations."[68] In this aside, they explained that "[w]illful public defamation of an individual can be a traumatic experience which deserves to be taken as seriously as" threats, harassment and disorderly conduct, all of which were criminalized by the Code.[69]

The Supreme Court quoted the drafters of the Model Penal Code approvingly in 1964, when it decided *Garrison v. Louisiana.*[70] The case involved a criminal libel prosecution brought against Garrison, a Louisiana prosecutor who had criticized the criminal court judges in the Louisiana parish where he practiced.[71] Garrison was tried and convicted of violating the state's criminal libel statute, which made it a crime for anyone to maliciously publish material that "expose[d] any person to hatred, contempt, or ridicule, or . . . deprive[d] him of the benefit of public confidence or social intercourse."[72] He appealed, and the Supreme Court held that the Louisiana statute violated the First Amendment.[73]

The Court began its analysis of the statute by citing its decision in *New York Times Co. v. Sullivan,*[74] which involved a First Amendment challenge to a civil libel statute. An Alabama official had brought a civil libel suit against the *New York Times,* seeking damages for allegedly defamatory statements made in an advertisement published in the paper.[75] The official won a judgment in the trial court that was then upheld by two Alabama appellate courts.[76] The Supreme Court reversed because it found the Alabama law violated the First Amendment.[77] More precisely, the Court found that a law allowing the imposition of civil damages upon those who criticized public officials would deter political speech protected by the First Amendment; it also found that Alabama's recognizing truth as a defense to the imposition of such liability was insufficient to control the chilling effect resulting from the possibility of liability like that imposed on the *New York Times*.[78] The *Sullivan* Court held, therefore, that the First Amendment requires that a public official be precluded "from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not."[79]

---

[66] *Id.* They also cited First Amendment concerns. *See id.* at 45.

[67] *See id.* at 45-46.

[68] *Id.*

[69] *Id.*

[70] 379 U.S. 64, 69-70 (1964).

[71] *Id.* at 65-66.

[72] *Id.* at 65 n.1 (quoting LA. REV. STAT. ANN. § 14:47 (1950)); *see also supra* Part II.A.

[73] *See Garrison*, 379 U.S. at 77-78.

[74] 376 U.S. 254 (1964).

The *Garrison* Court held that the *Sullivan* rule applies to prosecutions for criminal libel when the statements at issue in the prosecution relate to the conduct of public affairs.[80] It found "no merit in the argument that criminal libel statutes serve interests distinct from those secured by civil libel laws, and therefore should not be subject to the same limitations."[81]

---

[75] *Id.* at 256-58.

[76] *Id.* at 262-64.

[77] *Id.* at 264.

[78] *See id.* at 275-80.

[79] *Id.* at 279-80.

[80] *See* Garrison v. Louisiana, 379 U.S. 64, 71-74, 77-78 (1964). The *Garrison* Court left open the issue as to whether the *Sullivan* rule also applies "where purely private libels, totally unrelated to public affairs, are concerned." *Id.* at 72 n.8. The Court has so far never resolved this issue. *See* Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975). It has, as one scholar noted, "not completely foreclosed defamation liability for all true speech, such as true but defamatory speech about private individuals and private subjects." Carol Rice Andrews, Jones v. Clinton*: A Study in Politically Motivated Suits, Rule 11, and the First Amendment*, 2001 BYU L. REV. 1, 77 n.320 (2001).

[81] *Garrison*, 379 U.S. at 67. The Court cited the commentary to the Model Pe-

The *Garrison* Court cited history for the proposition that the common law breach of the peace justification for criminalizing libel had no applicability in the twentieth century,[82] and quoted the drafters of the Model Penal Code for the proposition that no other compelling considerations justify prosecutions for criminal defamation.[83]

D. Assessment

The failure to include a criminal libel provision in the Model Penal Code, coupled with the Court's decisions in *Sullivan* and *Garrison*, seemed to indicate there was neither an empirical need nor a constitutional basis for criminalizing defamation.[84] Some scholars therefore conclude that criminal libel has fallen into a state approaching extinction,[85] but others disagree.[86] The first group cites the relative paucity of state criminal libel statutes as proof that the crime is no longer taken seriously; the second group cites the persistence of such statutes as evidence that it is.[87]

As far as this article is concerned, it really does not matter

---

nal Code for this proposition and, in so doing, implicitly adopted its underlying rationale, *i.e.*, that civil liability suffices to control defamation. *See id.* at 69-70; *see also supra* note 68 and accompanying text.

[82] *See Garrison*, 379 U.S. at 69; *see also* Ashton v. Kentucky, 384 U.S. 195, 199-200 (1966) (in holding that a common law criminal libel offense was void for vagueness, the Court noted that basing a crime on the premise that conduct is likely to create a breach of the peace "'makes a man a criminal simply because his neighbors have no self-control and cannot refrain from violence'") (quoting Zechariah Chafee, FREE SPEECH IN THE UNITED STATES 151 (1954)).

[83] *See Garrison*, 379 U.S. at 69-70.

[84] *See, e.g.,* Tollett v. United States, 485 F.2d 1087, 1094 (8th Cir. 1973).

[85] Mark W. Freel, Note, *Grand Jury Subpoenas and the Threat to Free Speech:* In re Grand Jury Matter (Gronowicz), 18 CONN. L. REV. 665, 684 n.109 (1986).

[86] *See, e.g.*, Clive Walker, *Reforming the Crime of Libel,* 50 N.Y.L. SCH. L. REV. 169, 197 (2005-2006) ("[T]he perception of a constitutionally inspired 'death blow' to . . . criminal libel . . . is belied by the survival of the crime in twenty-five states and territories.") (citing David A. Elder, Defamation: A Lawyer's Guide para. § 4.5 (1993)); Lisby, *supra* note 26, at 455-56.

[87] *Compare* David Kohler, *Forty Years After* New York Times v. Sullivan: *The Good, the Bad, and the Ugly*, 83 OR. L. REV. 1203, 1232-33 (2004) *with* Walker, *supra* note 86, at 197.

which group is correct. We are concerned not with what criminal libel *is*, but with whether it should *become* a tool societies use to control certain types of online speech. The differentiating factor in this analysis is our focus on cyberspace—on the virtual publication of content that may, or may not, be sufficiently objectionable to warrant the imposition of criminal liability. The goal of the analysis is to assess the need for such a tool, to evaluate the extent to which the significance of online publication is a differentiating factor that merits, indeed, requires, the resuscitation and expansion of criminal libel.

To determine if criminal libel should become a tool societies use to control certain types of online speech, we must examine several issues. The first is whether online publication truly inflicts new harms that exceptionally disturb our collective sense of security. If we conclude it does not, our inquiry is at an end; if, on the other hand, we conclude that online publication does inflict new harms, we must determine whether the imposition of civil liability on those who are responsible for the infliction of these harms is sufficient to control this type of online speech. If we decide that the use of civil liability suffices even in the online context, the analysis ends there; if we decide it does not suffice in this context, then we will have to consider whether, and how, criminal liability should be used to keep online speech within socially acceptable bounds.

The next two sections examine these issues. Part III explains how cyberspace can be used to disseminate defamatory material; it provides an empirical foundation for the analysis presented in Part IV. Part IV evaluates the need for, and the propriety of, using criminal defamation to control online speech.

III. DEFAMATION IN CYBERSPACE

This section demonstrates how cyberspace can be used to disseminate defamatory speech; it provides an empirical foundation for the analysis in Part IV. Part III(A) refines the focus of that analysis, while Part III(B) examines some representative cases in which cyberspace was used to distribute speech that some, at least, found unacceptable for varying reasons.

A. Focus

Before we examine online publication of defamatory material, we need to (i) note a caveat and (ii) review the assumptions that are responsible for the current state of affairs in which criminal libel is, to say the least, disfavored by American law.

The caveat goes to the scope of this discussion: The Internet has made it possible for basically anyone to disseminate a wide variety of speech, some of which may disturb the person it concerns; speech can be disturbing for many reasons, only one of which is that it qualifies as defamatory.[88] This article, however, is exclusively concerned with speech that is defamatory, as defined above;[89] it therefore does not deal with online speech that is harassing, threatening or disturbing for other reasons.[90]

The assumptions that created the current state of affairs shape the focus of the analysis presented in Part IV. As explained above, criminal libel is disfavored in American law for two reasons: The drafters of the Model Penal Code concluded, forty-five years ago, that the harm defamation inflicts is *generally* not sufficient to warrant the imposition of criminal liability given the availability of civil redress; and the Supreme Court concluded, forty-two years ago, that the common law breach of the peace justification does not apply in the modern world and there was no other compelling justification for criminalizing defamation.[91]

Both entities based their conclusions on an empirical reality that was as yet unaffected by modern communication technology.[92] The drafters of the Model Penal Code and the Justices who decided the *Sullivan* and *Garrison* cases wrote in an era when publication in the generic sense—disseminating content to a broad audience—was a bounded phenomenon.[93] Forty years ago, the only venues for publication were the MSM: radio, television, cinema and print media (books, magazines, newspapers). This is significant for two reasons.

---

[88] For a definition of defamatory speech, see *supra* Part II.A.

[89] *See supra* Part II.A.

[90] For an analysis of other types of disturbing speech, see Brenner, *Complicit Publication, supra* note 29.

[91] *See supra* Part II.C.

[92] For more on this issue, see *infra* Part III.C.

First of all, the drafters of the Model Penal Code and the *Garrison* and *Sullivan* Justices both relied on the premise that the imposition of civil liability would redress the injury to the victims of defamation.[94] In so doing, they wrote on the slate they knew; that is, they assumed a world in which the responsibility for publication necessarily lay with a deep-pocket corporate entity.[95] It was consequently reasonable for them to assume that if a victim of defamation established the elements of civil liability, she *could* recover damages from the party responsible for publishing the defamatory material.[96] This, they assumed, would not only redress the injury to the victim, it would also create a financial disincentive that would discourage other corporate entities from publishing defamatory material and effectively control the dissemination of such material.[97] The latter assumption—the disincentive assumption—is not articulated either in the Model Penal Code commentary or the majority opinions in *Sullivan* or *Garrison*.[98] It is inferentially derivable from both because the drafters of the Model Penal Code concluded that the "community's sense of security" could be maintained without criminalizing defamation, and the *Garrison* Court quoted this conclusion with approval.[99]

---

[93] The circumscribed definition of publication given in Part II(A) is specific to defamation law. In law, as elsewhere, publication is more generally understood as being the act of distributing content to a wide audience—to the public. *See, e.g.*, BLACK'S LAW DICTIONARY 1264 (8th ed. 2004) (defining publication as "[t]he offering or distribution of copies of a work to the public"); *see also* THE CHAMBERS DICTIONARY 1221 (9th ed. 2003) (defining publication as "the act of publishing or making public; a proclamation").

[94] *See supra* note 81 and accompanying text. *See also supra* Part II.C.

[95] The defamatory materials at issue in *Sullivan* and in *Garrison* were published by newspapers with wide circulations. *See* New York Times v. Sullivan, 376 U.S. 254, 256-258 (1964); Brief of Appellee, Garrison v. Louisiana, 379 U.S. 64 (1964) (No. 4); *see also* Farmers Educ. & Coop. Union v. WDAY, Inc., 360 U.S. 525, 526 (1959); Polizzi v. Cowles Magazines, Inc., 345 U.S. 663, 664 (1953); *cf.* Ashton v. Kentucky, 384 U.S. 195, 196 (1966) (involving a criminal libel charge based on a pamphlet "which had a limited circulation").

[96] This assumption that victims *could* obtain redress by bringing a civil suit is one of the factors the Supreme Court cited in rejecting the breach of the peace justification for criminal libel. *See Garrison*, 379 U.S. at 69; *see also supra* Part II.C.

[97] *Garrison*, 379 U.S. at 69.

The fact that the Model Penal Code commentary and the *Sullivan* and *Garrison* opinions were written in a world in which publication was controlled by MSM is significant for a second reason. MSM domination of the available venues for publication imported an element of control that limited the opportunities for, and the incidence of, defamation.[100] It also tended to mitigate the virulence of the material that was published.[101] Media control of the agencies of publication prevented excess and effectively kept defamation within socially acceptable bounds.

As many have noted,[102] cyberspace has fundamentally altered the reality that gave us the Model Penal Code and the *Sullivan* and *Garrison* decisions. Before we assess the need to revisit the Code drafters' and the Court's rejection of criminal libel, we need to review precisely the extent to which the Internet has affected publication in general and defamatory publication in particular.

---

[98] *See supra* Part II.C.

[99] *See supra* Part II.C.

[100] Much, but not all, of this control resulted from the financial disincentives noted in the text above. Aside from the business considerations that prompt media to avoid publishing defamatory material, members of the MSM have voluntarily adopted ethical standards that are intended to maintain accuracy and, insofar as possible, preserve privacy. *See, e.g.*, Society of Professional Journalists, Code of Ethics (1996), *available at* http://www.spj.org/ethics_code.asp; Radio-Television News Directors Association and Foundation, Code of Ethics and Professional Conduct (2000), *available at* http://www.rtnda.org/ethics/coe.shtml; British Broadcasting Corporation, Editorial Guidelines (2005), *available at* http://www.bbc.co.uk/guidelines/editorialguidelines/edguide/.

[101] *See supra* note 100 and accompanying text.

[102] *See, e.g.*, *supra* note 1 and accompanying text.

B. *Online Publication of "Problematic" Speech*

Our focus in this article is on the legal concept of defamatory speech. MSM control of publication tended to keep defamatory speech within certain predictable bounds until the end of the twentieth century,[103] when cyberspace began to become a popular theater of human activity. One of the things cyberspace has done is to give anyone with access to the Internet the ability to become a publisher—an online publisher.[104] This has vastly expanded the opportunities for the publication of what we will call "problematic" speech.

Defamation is a legal construct and, as such, bundles a fixed set of denotations and connotations;[105] if we were to limit our review of online publication to defamatory content, we would overlook much of what many regard as problematic speech. Problematic speech is, for lack of a more precise definition, speech some (many) find unacceptable for varying reasons.

Cyberspace is so extensive and so fluid that it is impossible to describe all of the ways in which speech can be problematic. The sections below summarize some of the more egregiously problematic varieties of online speech. The categories are illustrative and, as such, are not immutable; the activity described in one may also inflict harm of the type at issue in another category. The purpose is merely to illustrate some of the ways in which online speech can be problematic.

1. Ridicule

> *"[T]hat's the problem with the Internet. Things travel fast."*[106]

---

[103] *See supra* Part III.A.

[104] *See, e.g.*, John R. Suler, *Publishing Online: Idea Independence, Interdependence, and the Academic*, *in* THE PSYCHOLOGY OF CYBERSPACE (1996), http://www.rider.edu/suler/psycyber/psycyberublish.html.

[105] *See supra* Part II.A.

[106] Tu Thanh Ha, *"Star Wars Kid" Cuts a Deal with His Tormentors*, GLOBE & MAIL, Apr. 7, 2006, *available at* http://www.theglobeandmail.com/servlet/story/RTGAM.20060407.wxstarwars07?BNStory/National/home (quoting Jerome Laflamme) (emphasis added). Laflamme was involved in distributing the *"Star Wars* Kid" video. *See id.*; *see also infra* notes 110-13 and accompanying text.

Last summer, Kim Hyo-bi, a twenty-two year old student in South Korea, discovered her picture had been posted "on a photo-sharing website . . . with her face colored and distorted to make her look silly, titled alongside the original as 'Before and After.'"[107] After the photos were posted, she "was barraged with calls from friends who saw the page, and the humiliation and feeling of being violated caused her several sleepless nights."[108] She remains "keenly aware of any cameras around her" and reacts irritably when she knows she is being photographed.[109]

A more notorious incident of ridicule involved Ghyslain Raza, a Canadian high-school student who videotaped himself pretending to be a *Star Wars* character wielding a light saber and then left the tape in the machine.[110] His classmates found the tape and uploaded it to a file-sharing site; the tape, which was subsequently, and repeatedly, enhanced with music and special effects, was viewed millions of times and Raza became famous as the less than agile "*Star Wars* Kid."[111] According to Raza, the release of the tape made life "'unbearable'" for him at school because classmates mocked him; he left school, but was tormented by people's recognizing him as the "*Star Wars* Kid."[112] Suffering from depression and other problems caused by the tape's release, Raza eventually sued the students who put it online.[113] Three years later, he settled with them; the details of the settlement, including whether it involved "monetary compensation," were not revealed.[114] It was never clear if the parents of the students he sued had insurance or other assets that could have been used to pay the damages Raza sought.[115] Raza's tape is still available online,[116] and there appears to be absolutely nothing he can do to remove it.

---

[107] Yu Sup Lee, *"Cyberviolence" Plagues South Korea*, USA TODAY, Mar. 8, 2006, http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-cyberviolence-south-korea_x.htm.

[108] *Id.*

[109] *Id.*

[110] Associated Press, *"Star Wars Kid" Becomes Unwilling Internet Star*, USA TODAY, Aug. 21, 2003, http://www.usatoday.com/tech/webguide/internetlife/2003-08-21-star-wars-kid_x.htm.

[111] *See* Ha, *supra* note 106.

[112] *Id.* (quoting Ghyslain Raza, *Star Wars* Kid).

[113] *Id.* It is not clear precisely what cause(s) of action Raza invoked in his suit.

[114] *Id.*

2. Invasion of Privacy

> *"It is one thing to be manipulated and used by a lover, it is another thing to be cruelly exposed to the world."*[117]

In May of 2004, Robert Steinbuch, a staff attorney for Ohio Senator Mike DeWine, met Jessica Cutler, a DeWine staffer, at a bar and "[t]hey apparently hit it off. A few hours later, Cutler and Steinbuch went to her apartment and enjoyed sexual activities."[118] Their sexual encounters continued over the next twelve days, during which Cutler described the details (such as the fact that Steinbuch liked to spank and to be spanked) of their encounters in postings on her blog.[119] The postings remained obscure until they were picked up by the popular blog Wonkette, "and the entire world quickly learned" the intimate details of the Cutler-Steinbuch affair.[120] This put a dramatic end to the affair, and a year later Steinbuch sued Cutler, asserting that her "'cruel and malicious exposures' entitled him to substantial compensatory and punitive damages under two invasion of privacy liability theories (false light and disclosure of private facts)."[121]

---

[115] *Id.*

[116] *See, e.g.,. Star Wars Kid*, http://www.jedimaster.net/.

[117] Complaint at 20, Steinbuch v. Cutler, 2006 WL 3060084 (D. D.C. Oct. 30, 2006) (No. 05-0970(PLF)) (emphasis added).

[118] Bruce Johnson, Steinbuch v. Cutler*: When is a Personal Blog Considered Publicity*, Privacy and Security Law Blog, Mar. 29, 2006, http://www.privsec.blog.com/archives/blogging-steinbuch-v-cutler-when-is-a-personal-blog-considered-publicity.html (last visited Feb. 10, 2007).

[119] *Id.*

[120] *Id.*

[121] *Id.* (citing Complaint at 20, Steinbuch v. Cutler, 2006 WL 3060084 (D. D.C. Oct. 30, 2006) (No. 05-0970(PLF))). Steinbuch's claims for invasion of privacy were based on the Restatement of Torts (Second) § 652D (1977). Tort law recognizes a

---

cause of action for such invasions: One who publicizes "a matter concerning the private life of another" can be held civilly liable "if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (1977); *see, e.g.*, Motion to Dismiss at 16-17, Steinbuch v. Cutler, 2006 WL 3060084 (D. D.C. Oct. 30, 2006) (No. 05-0970(PLF)).

The Model Penal Code includes a provision criminalizing certain invasions of privacy. *See* MODEL PENAL CODE § 250.12 (1962). The first section of the provision criminalizes eavesdropping or visual surveilling "in a private place." *Id.* at § 250.12(1). The eavesdropping or surveillance can be accomplished in person or by electronic means. *See id.* Ohio, South Carolina and Utah have codified versions of this provision. *See* OHIO REV. CODE ANN. § 2907.08 (2003 & Supp. 2005); S.C. CODE ANN. § 16-17-470 (2003); UTAH CODE ANN. § 76-9-402 (2003). The second section of the Model Penal Code provision makes it a misdemeanor to intercept and/or disclose the contents of a private message. *See* MODEL PENAL CODE § 250.12(2) (1962). Washington has codified this provision, while North Carolina adopted a version making it a crime to "violate the privacy" of telegrams. *See* N.C. GEN. STAT. § 14-371 (2005); WASH. REV. CODE ANN. §§ 9.73.010 & 9.73.020 (2003).

A few states have criminalized invasion of privacy, but they do not seem to have followed the Model Penal Code in this regard. Colorado, for example, defines "criminal invasion of privacy" as taking "a photograph of another's intimate parts" without their consent. COLO. REV. STAT. § 18-7-801(1) (2005). A few other states have similar provisions. *See* DEL. CODE ANN. tit. 11, § 1335 (2002); HAW. REV. STAT. ANN. § 711-1110.9 (LexisNexis 1993 & Supp. 2005); ME. REV. STAT. ANN. tit. 17-A, § 511 (2006). Iowa has a somewhat analogous provision, which defines invasion of privacy as viewing, photographing or filming someone without their consent while they are in a state of full or partial nudity. IOWA CODE ANN. § 709.21 (West 2003 & Supp. 2005). Idaho, Indiana, Kentucky, Michigan, Mississippi, Missouri, New Hampshire, Oregon, Pennsylvania, Rhode Island, Vermont, Washington, West Virginia and Wisconsin have similar provisions. *See* IDAHO CODE ANN. § 18-6609 (2004); IND. CODE § 35-44-1-4.5 (2004); KY. REV. STAT. ANN. § 531.090 (West Supp. 2004); MICH. COMP. LAWS ANN. § 750.539j (West 2004); MISS. CODE ANN. § 97-29-63 (2006); MO. ANN. STAT. §565.252 (West Supp. 2005); N.H. REV. STAT. ANN. § 644:9 (1996); OR. REV. STAT. ANN. § 163.700 (West 2001); 18 PA. CONS. STAT. ANN. § 7507.1 (West 2000 & Supp. 2005); R.I. GEN. LAWS § 11-64-2 (2002 & Supp. 2004); VT. STAT. ANN. tit. 13, § 2605 (1998); WASH. REV. CODE ANN. § 9A.44.115 (West 2000 & Supp. 2005); W. VA. CODE § 61-8-28 (2005); WIS. STAT. ANN. § 942.08 (West 2005). Other states have similar provisions that criminalize "voyeurism." *See, e.g.*, ARK. CODE ANN. § 5-16-102 (2006); CONN. GEN. STAT. ANN. § 53a-189a (West 2001 & Supp. 2005); FLA. STAT. ANN. § 810.14 (West 2000); LA. REV. STAT. ANN. §§ 14:283-283.1 (2004 & Supp. 2006); WYO. STAT. ANN. § 6-4-304 (2005).

A very few states make "computer invasion of privacy" a crime, but these provisions are really computer crime statutes, in that they are concerned with preventing unauthorized intrusions into computer systems rather than violations of the personal privacy of an individual. *See* VA. CODE ANN. § 18.2-152.5 (2004 &

By the spring of 2006, Steinbuch's suit had survived a motion to dismiss and was proceeding to discovery.[122] Even if he prevails, it is unlikely Steinbuch can collect from Cutler, who has changed lawyers several times due to her apparent inability to pay legal fees.[123] Even the judge questioned the wisdom of filing suit: "'I don't know why this guy thought it was smart to file a lawsuit and lay out all of his private intimate details in an appendix to the complaint.'"[124] Steinbuch is apparently determined to "set the record straight" about details such as "whether he is able to ejaculate with or without a condom or whether he likes to spank or be spanked."[125]

A similar but perhaps more compelling incident involved Virginia Congressman Edward Schrock who "abruptly dropped out of his race for a third term" after gay activist Michael Rogers claimed on a website that Schrock is gay.[126] Rogers' online "outing" of Schrock included posting an "audio file of Congressman Schrock seeking gay sex off of gay sex lines."[127]

Supp. 2005); W. VA. CODE § 61-3C-12 (2005).

As this survey demonstrates, most of the state statutes that criminalize "invasions of privacy"—however defined—are voyeurism provisions. That is, they criminalize the act of "spying on" another, usually for the purpose of gaining "sexual pleasure." *See, e.g.*, BLACK'S LAW DICTIONARY 1167 (8th ed. 2004) (defining "Peeping Tom"); *see also id.* at 1609 (defining "voyeur"). The remaining statutes, like the Model Penal Code provision, derive from the common law crime of eavesdropping, which targeted the harm of violating the privacy of someone's home. *See* WILLIAM BLACKSTONE, 4 COMMENTARIES *168; *see also* Note, *The Right to Privacy in Nineteenth Century America,* 94 HARV. L. REV. 1892, 1896 (1981).

[122] *See* Steinbuch v. Cutler, No. 05-0970(PLF), 2006 WL 3060084 (D.D.C. Apr. 14, 2006) (mem.).

[123] T.R. Goldman, *A Man Scorned*, LEGAL TIMES, May 22, 2006, http://www.law.com/jsp/dc/PubArticleDC.jsp?id=1147943130871&hub=TopStories.

[124] *Id.* (quoting U.S. District Judge Paul Friedman).

[125] *Id.*

[126] Michael D. Shear & Chris L. Jenkins, *Va. Legislator Ends Bid for Third Term: Schrock Cites Unspecified Allegations Questioning His Ability to Serve*, WASH. POST, Aug. 31, 2004, at A02, *available at* http://www.washingtonpost.com/wp-dyn/articles/A47194-2004Aug30.html.

[127] Posting of Michael Rogers to BlogActive, *Schrock Faces Accusations: Cancels Congressional Campaign*, http://www.blogactive.com/2004/08/schrock-faces-accusations-cancels.html (Aug. 30, 2004). This article will assume, for the purposes of analysis *only*, that Rogers' "outing" of Schrock was based on accurate information. This assumption will come into play later, when we consider the role, if any,

3. False Light

"It destroys our reputations."[128]

A case from Wisconsin illustrates how someone can use cyberspace to cast another in a seriously "false light."[129] After his boss fired him, David Dabbert went to the "Sex on the Side" website, which "features 'attached' women who are seeking sexual encounters 'on the side.'"[130] Dabbert posted an advertisement on the site that purportedly came from his former boss, using her real name and email address.[131] The ad "described her chest size and hair color and, in part, said: 'I'm highly stressed out. . . . I've only been with my hubby. He's gone at work 24 hours at a time . . . I want someone to make me their slut for the night.'"[132] The woman received many responses to the advertisement, which left her frightened and embarrassed.[133]

In a similar case, "a family therapist posed as his former wife's new husband and posted an ad on an Internet site for swingers, asking interested men to call the couple."[134] It gave "the ex-wife's body measurements and home phone number and

---

privacy claims should play in our defamation analysis. *See infra* Part IV.A.

[128] Katie Dean, *Do "Dissed" Teachers Have Case?*, WIRED NEWS, June 12, 2000, http://www.wired.com/news/culture/0,1284,36720,00.html (quoting Daniel Curzon-Brown) (emphasis added). Curzon-Brown sued a website for posting what he believed were defamatory comments about his teaching. *See infra* notes 143-47 and accompanying text.

[129] Tort law recognizes a cause of action for portraying another in a false light, *i.e.*, for placing someone "before the public in a highly offensive and untrue manner." BLACK'S LAW DICTIONARY 636 (8th ed. 2004) (defining false light); *see* RESTATEMENT (SECOND) OF TORTS § 652E (1977). There seems to have been no attempt to criminalize false light, at least not in this sense.

[130] Lisa Sink & Linda Space, *Man Charged with Defamation: Disgruntled Fired Employee Accused of Posting Ad with Ex-boss' Name on Internet*, MILWAUKEE J. SENTINEL, June 7, 2000, at 1B; *see* The World Famous Sex on the Side Club, http://www.sex-on-the-side.org/index.html (last visited Jan. 14, 2007).

[131] Sink & Spice, *Man Charged with Defamation*, *supra* note 130.

[132] *Id.* (citing criminal complaint against Dabbert).

[133] *Id.*

[134] Lisa Sink, *Family Therapist Investigated in Internet Complaint; Phone Number of Former Wife, Her New Husband Posted in Swingers Ad*, MILWAUKEE J. SENTINEL, Mar. 14, 2000, at 1B.

said: 'Wife and I desire [three]some with a male. . . . '"[135] The advertisement "prompted a slew of calls to the woman and her new husband," which, again, left them frightened and embarrassed.[136]

There are many other ways cyberspace can be used to cast someone in a false light. Educators have been notably vulnerable to this kind of activity. In 1998, Glenda Miskin, then a student at the University of North Dakota (UND), published an article entitled *Kinky Torrid Romance by Randy Physics Professor* on the UND News website, a privately-operated venture that exposes alleged wrongdoing at the University.[137] In the article, Miskin accused Physics Professor John Wagner "of being a pedophile and [of] having odd sexual habits."[138] Outraged, Wagner sued Miskin for defamation and eventually won a judgment requiring her to pay him $3 million and apologize for the story.[139] Aside from establishing that the jury disbelieved her allegations,[140] the judgment was a purely Pyrrhic victory: Miskin could never pay such a sum; she declared, after the judgment issued, that she would not apologize; and her story was available online long after the jury returned its verdict.[141] Wagner paid his own attorney fees, recovering nothing from Miskin.[142]

---

[135] *Id.* The ad may have been prompted by a custody dispute between the former spouses. *See id.*

[136] *Id.*

[137] Scott Carlson, *Former Student's Online Accusations Against Professor Prompt Libel Suit*, CHRON. OF HIGHER EDUC., Dec. 7, 2000, http://chronicle.com/free/2000/12/2000120701t.htm; *see also* UND News, About Us, http://www.undnews.com/main/aboutus.htm. At the time, Miskin owned and operated the UND News website. Scott Carlson, *Former Student's Online Accusations Against Professor Prompt Libel Suit*, CHRON. OF HIGHER EDUC., Dec. 7, 2000, http://chronicle.com/free/2000/12/2000120701t.htm.

[138] Carlson, *Former Student's Online Accusations*, *supra* note 137; *see also* UND News, University of North Dakota, *J. L. Wagner: Career Misogynist*, http://www.undnews.com/university_of_north_dakota_j_l_wAGNER_CAREER_MISOGYNIST.htm (claiming that Wagner said "he 'likes' prepubescent children, their grandmothers, and great-grandmothers. He says that he does not do well with women his own age").

[139] Thomas Bartlett, *Physics Professor Wins $3 Million Judgment in Libel Suit Against Ex-Student*, CHRON. OF HIGHER EDUC., Apr. 4, 2002, http://chronicle.com/free/2002/04/2002040404n.htm.

[140] *See* N.D. Century Code § 14-02-03 (defining libel as a "false . . . publication"); *see also infra* Part IV.

In a somewhat analogous case, Daniel Curzon-Brown, an openly homosexual professor at City College in San Francisco, sued Ryan Lathouwers, founder and webmaster of Teacher Review, a site that "post[ed] anonymous comments about . . . faculty members."[143] Curzon-Brown sued for defamation after he was the subject of "postings that use[d] the word 'faggot' frequently, and allege[d] that he raped and molested students in exchange for better grades."[144] One posting claimed he had sex with a student in the classroom; another accused him of killing a student.[145] A year later, Curzon-Brown agreed to dismiss the suit and to pay the American Civil Liberties Union (ACLU) $10,000 in attorneys' fees; the ACLU represented Lathouwers, who could not afford private counsel.[146] Had Curzon-Brown not agreed to dismiss, the ACLU would have moved for dismissal on the grounds that Lathouwers was statutorily immune from suit under the Communications Decency Act of 1996, and would have sought $100,000 in attorneys' fees.[147]

---

[141] Bartlett, *supra* note 139; *see also* Robert Franklin, *Internet Posting Results in $3 Million Verdict; A Professor Won a Suit Against a Student Who Made Accusations Against Him on a Web Site*, STAR TRIB., Sept. 30, 2002, at 1B; Xiao Zhang, *Jury Awards UND Professor $3 Million in Defamation Case; Nine-Member Panel Also Demands Former Student Retract Articles, Apologize*, GRAND FORKS HERALD, Apr. 3, 2002, at B2.

[142] *See generally* Tom Bryan, *UND Prof Sues Web Site Creators; Names Student Editors, Service Providers of www.undfraud.com*, GRAND FORKS HERALD, Nov. 27, 2000, at A1 (Wagner's complaint sought attorney's fees).

[143] Scott Carlson, *Lawsuit Pits 2 Instructors Against Anonymous "Teacher Review" Postings*, CHRON. OF HIGHER EDUC., June 1, 2000, *available at* http://chronicle.com/cgi2-bin/printable.cgi?article=http://chronicle.com/free/2000/06/2000060101t.htm. Jesse David Wall, another City College faculty member, also sued. *Id.*

[144] *Id.*

[145] *See* Dean, *supra* note 128.

[146] Tanya Schevitz, *Teacher Review Web Site Escapes Suit; S.F. College Professors Drop Defamation Case*, S.F. CHRON., Oct. 4, 2000, at A17, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/10/04/MN83928.DTL. Wall agreed to the same terms. *See supra* note 143.

[147] Schevitz, *supra* note 146; *see also* Carlson, *Lawsuit Pits 2 Instructors*, *supra* note 143.

The Communications Decency Act "overrides the traditional treatment of publishers . . . 'such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing . . . obscene or defamatory material written or prepared by others.'"[148] Concerned about lawsuits inhibiting free speech online, Congress added section 230(c)(1) to title 47 of the U.S. Code.[149] It states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[150] The effect of this provision is to immunize those who, like Lathouwers, post content that is provided by another, such as the individuals who submitted the postings about Curzon-Brown.[151] At least one court has found that the immunity applies even though the operator of the site "exercises some editorial control over the anonymous postings."[152]

Curzon-Brown's experience illustrates the problems individuals can encounter in seeking civil redress from those who have contributed to the online distribution of defamatory material. If the author and publisher of the material are distinct, the aggrieved person may want to seek redress from either or both. The publisher is an obvious target, if only because he/she/it is readily identifiable. But as Curzon-Brown learned, the publisher of the material—the operator of the website on which it appeared—is immune from suit under the Communications Decency Act.[153] The publisher may also be, like Lathouwers and Miskin,[154] judgment-proof, *i.e.*, "unable to satisfy a judgment" for damages because he or she lacks assets and has a limited income.[155] This leaves the author of the posted material, but difficulties arise here as well. For one thing, the author may be anonymous; if the publisher does not know who the author is, the aggrieved party will probably be unable to identify and pursue him or her.[156] And even if the aggrieved party is able to identify the author of a defamatory posting, the author may be judgment-proof, like Miskin. We return to these issues in Part III(C).

---

[148] Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003) (quoting Blumenthal v. Drudge, 992 F.Supp. 44, 49 (D.D.C. 1998)).

[149] *See Batzel*, 333 F.3d at 1026-30.

[150] 47 U.S.C. § 230(c)(1) (2000).

[151] *See Batzel*, 333 F.3d at 1030-31.

[152] Shannon P. Duffy, *Judge: Bloggers Entitled to Immunity Under Communications Act*, LEGAL INTELLIGENCER, June 2, 2006, *available at* http://www.law.com/jsp/article.jsp?id=1149152717145 (analyzing the district court's opinion in the case of DiMeo v. Max, 433 F. Supp. 2d 523 (E.D. Pa. 2006)).

[153] *See* Carlson, *Lawsuit Pits 2 Instructors*, *supra* note 143.

[154] *See* Carlson, *Former Student's Online Accusations*, *supra* note 137. As noted earlier, Miskin was both the author of the posting about Wagner and the publisher of the UND News website. *See supra* notes 137-42.

4. Not-So-False Light

> *"If this guy Hoyt is not the one, God help us all for sullying the man's name."*[157]

The cases examined in Part III(B)(3) are categorized as false light cases because it is reasonably certain that the allegations at issue were, in fact, false. Sometimes, though, it is difficult to tell whether allegations are true or false; and individuals may object to the distribution of material concerning them even if it is not false, or is not entirely false.[158] This section reviews a few, hopefully representative instances in which individuals have taken issue with the online dissemination of information and/or allegations about them that may, or may not, be false.

Our first example is the Foxy Felon case: In 2005, The Smoking Gun website posted its second collection of "'foxy felon' mug shots."[159] The collection consisted of mug shots of women who had been convicted of crimes, along with information about their crimes and the punishment they received.[160] A year later, one of the women featured in the collection, Casey Hicks, threatened to sue The Smoking Gun if it did not excise her mug shot.[161] The precise basis for the threatened litigation was not clear, but it seems to have included a defamation theory.[162] This is interesting because Hicks did not—and presum-

---

[155] BLACK'S LAW DICTIONARY 861-62 (8th ed. 2004) (defining "judgment-proof").

[156] *Cf.* Course Reviews.com, Guidelines for Posting Reviews, http://www.coursereviews.com/help/guidelines (last visited Jan. 14, 2007) (stating that the website's policy requires posters to provide their "real email address" and receive a "verification key" before they can post messages).

[157] Kathryn Belgiorno, *The 21st-Century Peep Show*, VILLAGE VOICE, Apr. 25, 2006, available at http://www.villagevoice.com/news/0617,belgiorno,72978,6.html (quoting Posting of Unknown Author to http://www.gothamist.com/) (emphasis added). For the Hoyt story, *see infra* notes 172-74 and accompanying text.

[158] Objections to the dissemination of not-false or not entirely false information are usually predicated on an invasion of privacy theory. *See supra* Part III.B.2; *see also supra* note 121.

[159] *See* TheSmokingGun.com, Foxy Felons, http://www.thesmokinggun.com/ar-

---

chive/morehotfelons1.htmlhttp://www.thesmokinggun.com/archive/morehotfelons2.html (last visited Jan. 7, 2007). The Smoking Gun had apparently posted the collection several years before and reprised it in 2005. *See* TheSmokingGun.com, Foxy Felons, http://www.thesmokinggun.com/archive/hotfelon1.html (last visited Jan. 14, 2007).

[160] *See* TheSmokingGun.com, Foxy Felons, http://www.thesmokinggun.com/archive/morehotfelons1.htmlhttp://www.thesmokinggun.com/archive/morehotfelons2.html (last visited January 14, 2007).

The Smoking Gun packaged the mug shots and offense information of the Foxy Felons before posting it online. This at least somewhat differentiates what The Smoking Gun did from what an Ohio judge is doing. In June of 2006, Medina County Judge James Kimbler began "uploading his weekly sentencing hearings on the free video Web site YouTube.com." *Ohio Judge Broadcasts Sentencings on YouTube.com*, COLUMBUS DISPATCH, June 21, 2006, *available at* http://www.columbusdispatch.com/news-story.php?story=194030. Judge Kimbler does not appear in the videos; only the defendant, the defendant's attorney and what seems to be a bailiff appear in them. *Id.* While it is probably unlikely that any of the defendants will challenge what Judge Kimbler is doing, the practice might raise issues analogous to those under consideration in this article. The defendants could not, of course, claim that their privacy is being violated because the video records a public proceeding. Nor, since they have pled guilty to the charges against them, could they claim they are being cast in a false light. They might argue that this represents an impermissible *incremental* intrusion on their privacy: That is, while the sentencing itself is a public proceeding, sentencings are, traditionally, accessible to only a small, local audience. By uploading the video of a sentencing onto YouTube.com, Judge Kimbler is publishing it to a broader audience, which might well have negative effects that would not manifest themselves if the sentencing were available only to those who could attend in person.

[161] *See* TheSmokingGun.com, Foxy Felon Threatens TSG: Lawyer Claims Some Web Fans Get Their Kicks Leering at Ms. Hicks, http://www.thesmokinggun.com/archive/0221061hicks1.html (last visited Jan. 14, 2007); *see also* Letter from Terry D. Bork, Attorney for Casey Hicks, Harris, Guidi, Rosner, Dunlap, Rudolph & Catlin, P.A. to Thomas Fitzharris, Registered Agent, Courtroom Television Network, LLC (Feb. 13, 2006), *available at* http://www.thesmokinggun.com/archive/0221061hicks2.html (last visited Jan. 14, 2007).

[162] *See* Letter from Terry D. Bork to Thomas Fitzharris, *supra* note 161 (noting that the picture was meant to "hold her up to public ridicule and humiliation"); *supra* note 18 and accompanying text. Bork's letter also cited invasion of

ably could not—challenge the accuracy of what was posted.[163] Her defamation claim, insofar as one exists, seems to go to the issue of packaging, *i.e.*, to the fact that The Smoking Gun took information from the files of a public agency, assembled it with other information obtained from the same source and then posted all of the information online under a particular rubric, "Foxy Felons."

We are left to speculate about the nature of the injury Hicks believes she suffered: Does she feel defamed because the site characterized her as (i) "foxy" or (ii) a "felon?" Since she was convicted of possessing a controlled substance, the latter characterization seems factually unobjectionable; it is matter neither of opinion nor speculation. Any conclusions we might draw as to her reaction to the second characterization would be rampant speculation, so we will move on to what, inferentially, seems to be the real gist of Hicks' defamation claim: Essentially, she is complaining that The Smoking Gun took information which was concededly public—in a very limited fashion—and made it truly public by broadcasting it on the Internet. This distinguishes her defamation theory from the invasion of privacy cases we examined in Part III(B)(2). The site that "outed" Congressman Edward Schrock revealed information that was not in the public domain and, in so doing, arguably violated his right to maintain control over his private life.[164] Hicks' mug shot, conviction and sentence, on the other hand, were already a matter of public record, although the record was, and presumably would have remained, obscure. Absent The Smoking Gun's posting the information online, one could have accessed it only by traveling to or contacting the courthouse where the information was securely filed away.

The notion that one is defamed, *i.e.*, exposed "to public

---

privacy and claimed that the posting both jeopardized Hicks' safety and had made her an object some individuals were using "for their own private sexual gratification." Letter from Terry D. Bork to Thomas Fitzharris, *supra* note 161.

[163] Bork's letter suggests that the criminal history provided for Hicks was incorrect. Letter from Terry D. Bork to Thomas Fitzharris, *supra* note 161.

[164] *See supra* Part III.B.2; *see also supra* note 121.

hatred, contempt, or ridicule"[165] when otherwise public information is distributed online, surfaces in many of the not-so-false light cases. Take the South Korean woman who refused requests to clean up after her dog when it defecated on the floor of the subway car in which they were riding.[166] Outraged, another passenger used his cell phone to photograph her and the dog and then posted the photograph on a popular Korean website.[167] "[W]ithin days, she had been identified and much of her personal information was exposed on the Internet."[168] Parody posters appeared online; people began to call the now-easily-recognizable woman the "dog-poop girl;"[169] and someone posted her photo on an online auction site with the caption, "'I'm selling dog poop.'"[170] According to one source, the woman, who was a student, "quit her university" because she had been "[h]umiliated in public and indelibly marked."[171]

In August of 2005, Thao Nguyen was riding on a New York subway train when another passenger, a man, began masturbating in front of her.[172] Nguyen took a picture of him with her cell phone and posted it on websites along with a description of what had happened:

> The *New York Daily News* published a front page article . . . about the incident and included the photo. . . . The story . . . received wide attention from newspapers . . . [as well] as several weblogs. Several people called the *Daily News* claim-

---

[165] *See supra* note 18 and accompanying text.

[166] Wikipedia, *Dog Poop Girl*, http://en.wikipedia.org/wiki/Dog_poop_girl (last visited Jan. 14, 2007).

[167] *Id.*

[168] *Id.*

[169] *Id.*; *see also* ParodyLab.com, http://pds.egloos.com/pds/1/200506/07/79/b00036579_16272588.jpg (last visited Jan. 14, 2007).

[170] *"Trial by Internet" Casts Spotlight on Korean Cyber Mobs*, CHOSUN IBO, July 8, 2005, *available at* http://english.chosun.com/w21data/html/news/200507/200507080017.html.

[171] Jonathan Krim, *Subway Fracas Escalates into Test of the Internet's Power to Shame*, WASH. POST, July 7, 2005, D01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html.

[172] *See* Wikipedia, *Dan Hoyt*, http://en.wikipedia.org/wiki/Dan_Hoyt (last visited Jan. 14, 2007).

> ing that they believed the man to be Dan Hoyt. . . . [O]ther women came forward alleging that Hoyt was the same man who had exposed himself to them on prior occasions.[173]

Hoyt eventually surrendered to police, pled guilty to one count of lewdness and was ordered to receive counseling.[174]

The Hoyt episode prompted seven New York City residents to create "Holla Back NYC," "a photoblog and grassroots initiative to . . . combat street harassment by posting photographs and narrative accounts of individuals' encounters with offenders."[175] Since "Holla Back NYC" is a blog, the site leaves the determination as to what constitutes street harassment to those who submit postings.[176] Some postings—photographic and otherwise—are ambiguous, while many are graphic.[177] Regardless of the accuracy with which the poster discerned an alleged harasser's intent, the subject of the posting is lumped in with men who were foolish or reckless enough to expose themselves (in one way or another) to a camera or cell phone.[178]

These examples all involve instances in which the behavior that became the topic of web publication was itself unambiguous (though the import of some of the behaviors reported on the "Holla Back" site may be open to dispute). Our final example deals with a site that also reports particular behaviors, but in this instance the reports are clearly filtered through, and shaped by, the emotions and perceptions of the person submitting the report(s).

---

[173] *Id.*

[174] *Id.*

[175] Wikipedia, *Holla Back NYC*, http://en.wikipedia.org/wiki/Holla_Back_NYC (last visited Jan. 14, 2007); *see* Holla Back New York City, http://www.hollabacknyc.blogspot.com/. The founders of "Holla Back" define street harassment as "a form of sexual harassment that takes place in public spaces." Holla Back New York City, Holla FAQ, http://hollabacknyc.blogspot.com/2005/10/hollafaq.html (Oct. 2, 2005, 12:46 PM).

[176] *See* Holla Back New York City, Holla FAQ, http://hollabacknyc.blogspot.com/2005/10/hollafaq.html (Oct. 2, 2005, 12:46 PM). "Holla Back" websites have since been started in Seattle, Boston, and Washington, D.C., as well as in Texas, Canada, and Europe. *See* Holla Back New York City, Holla Back WORLD!, http://www.hollabacknyc.blogspot.com/.

[177] *See* Belgiorno, *supra* note 157; *see also* Posting of Emily to HollabackNYC, http://hollabacknyc.blogspot.com/2006_05_01_hollabacknyc_archive.html (May 25, 2006, 11:36 PM); Posting of HollaBackNYC to HollaBackNYC, http://hollabacknyc.blogspot.com/2005/10/holla-shame.html (Oct. 4, 2005, 10:25 AM).

[178] *See* Belgiorno, *supra* note 157 ("Is Tex a jackass who is about to take a piss? [O]r a jackass who . . . willfully exposed himself?"). "Holla Back NYC" does not accept postings from men who claim to have been sexually harassed by women. *See* Holla Back New York City, Holla FAQ, http://hollabacknyc.blogspot.com/2005/10/hollafaq.html (Oct. 2, 2005, 12:46 PM).

"Don't Date Him Girl" is a website where women can share their "relationship experiences with women around the globe."[179] According to the site, "[b]y adding your ex to DontDateHimGirl.com, you empower others with the knowledge to make an informed decision in a potential new love interest!"[180] Women who want to research a man can log on to the site and use a database to search for entries on that particular gentleman; some of the posts are, to say the least, highly critical of the men they focus on.[181] As this is written, the site is only five months old but reportedly has over 500,000 registered users and gets 600,000 hits a day.[182] Its Terms of Use section tells users they are "solely responsible" for the content they post, and that they should not post material that is "defamatory, inaccurate" or that violates another's right to privacy.[183]

Notwithstanding this warning, men featured on "Don't Date Him Girl" complain that its anonymous postings include material that is inaccurate or "partially true but twisted."[184]

---

[179] DontDateHimGirl.com, http://dontdatehimgirl.com/faqs/ (last visited Jan. 25, 2007). There are other similar sites. *See, e.g.*, WomanSavers.com, http://www.womansavers.com/.

[180] DontDateHimGirl.com, http://dontdatehimgirl.com/faqs/ (last visited Jan. 25, 2007).

[181] *See* DontDateHimGirl.com, http://dontdatehimgirl.com/search/cheater.asp?ddh_id=35881&return_url=index%2Easp%3F (last visited Jan. 25, 2007) ("This man is a liar and likes to play with ppl's [sic] emotions and I am here to tell the world and I hope he doesn't do this to you.. Please read this email he sent me, and you can see for yourself how he plays with ppl's [sic] minds") (emphasis omitted).

[182] Becky Thompson, *Web Site Exposes Cheaters, Bad Boyfriends: Women Seek Revenge Against Ex-Boyfriends*, WPXI.COM, May 17, 2006, http://www.wpxi.com/news/9234548/detail.html.

[183] DontDateHimGirl.com, Terms of Use, http://dontdatehimgirl.com/terms.html (last visited Jan. 14, 2007).

[184] Classaction-DontDateHimGirl.com, http://www.classaction-dontdatehimgirl.

Some of these complaints appear on an opposing website: Classaction-dontdatehimgirl.com offers "legal action information" about "Don't Date Him Girl" and posts comments from men who feel they have been harmed by information posted on the site.[185] In June of 2006, one man featured on "Don't Date Him Girl" decided to fight back: Pittsburgh attorney Todd Hollis announced he was going to sue Tasha Joseph, operator of Don't Date Him Girl, because his reputation is "being ruined by postings" on her site.[186] According to Hollis, entries allegedly posted by women who have dated him "accused him of giving them a disease, dating two people at a time and being bisexual or gay."[187] He says he cannot pursue his accuser(s) directly because he cannot identify them; as noted earlier, "Don't Date Him Girl" postings are anonymous.[188] Joseph responded by pointing out that she is immune from suit under the Communications Decency Act of 1996 and by suggesting that Hollis post a rebuttal, which she permits men to do on her website.[189]

Interestingly, between the time this article was written and the time the editorial process was completed, the tone of the "Don't Date Him Girl" site mellowed considerably.[190] We can only speculate as to why that is, but it seems reasonable to assume the change is due, at least in part, to the complaints about and litigation directed at the site.

---

com/ (last visited Jan. 14, 2007).

[185] *Id.*; *see, e.g.*, ClassAction-DontDateHimGirl.com, Howard M's Story, http://www.classaction-dontdatehimgirl.com/howardmstory.php.

[186] *Man Fights Back After Appearing on DontDateHimGirl.com: Local Man Says Entries Are False*, WPXI.COM, June 8, 2006, http://www.wpxi.com/news/9343498/detail.html.

[187] *Id.*

[188] *Id.*

[189] *Id.*; *see supra* notes 148-52 and accompanying text; *see also* DontDateHimGirl.com, Contact Us, http://www.dontdatehimgirl.com/contact_us/ (last visited Jan. 14, 2007) (explaining how to submit a rebuttal; however, the site does not remove profiles of the men in its database). *See* DontDatehimGirl.com, Search, http://www.dontdatehimgirl.com/search (last visited Jan. 14, 2007).

[190] *See, e.g.*, Thompson, *supra* note 182; DontDateHimGirl.com, http://dontdatehimgirl.com/faqs/ (last visited Jan. 25, 2007).

C. Online Publication Is Different

"Print publishing acts as a filter, weblogs do not."[191]

The drafters of the Model Penal Code made their decision not to criminalize defamation in a world in which there was only one model: real-world publication by the MSM (newspapers, magazines, books, radio, television and movies).[192] That model's reliance on professional staff discourages the publication of defamatory material by filtering the content of what is published in two ways.[193]

Most importantly, the real-world model filters the subject-matter of what is published. Because it is a commercial endeavor, MSM publication focuses on matters of general public interest, *i.e.*, topics that are likely to attract a large segment of the available audience.[194] One of the reasons the drafters of the

---

[191] Clay Shirky, *Weblogs and the Mass Amateurization of Publishing*, Oct. 3, 2002, http://shirky.com/writings/weblogs_publishing.html (emphasis added).

[192] *See supra* Part III.A. We will use the term "real-world" to denote activity—such as publication—that occurs solely in the "physical reality of everyday life which everyone experiences." Wikipedia, *Real World*, http://en.wikipedia.org/wiki/Real_world (last visited Jan. 14, 2007). The phrase "online publication" denotes the dissemination of information—text, sound, images, other data—by purely electronic means.

Defamation claims predicated on movie portrayals may not be as common as claims based on material published in the other components of the MSM, but they do arise. *See, e.g.*, *Film-maker Moore Facing Lawsuit*, BBC NEWS, July 15, 2004, http://news.bbc.co.uk/1/hi/entertainment/arts/3896011.stm.

[193] *See supra* notes 100-01 and accompanying text. MSM's default reliance on professional staff is attributable both to (i) MSM entities' conducting their respective operations as a business and (ii) the financial disincentives associated with the imposition of civil liability for the publication of problematic material. The first factor favors professionalism and the hierarchical organization that has historically proved advantageous in conducting commercial (and other) enterprises; utilization of professional staff and hierarchical organization are seen as effective ways to maximize an entity's competitiveness in the media marketplace. *See generally* Robert McChesney, *supra* note 5. The second factor promotes reliance on professional staff as a way to minimize financial losses attributable to successful and unsuccessful efforts to hold a media entity civilly liable for the publication of defamatory material. *See supra* notes 100-01 and accompanying text.

[194] *See, e.g.*, Steve Goodman, *An Open Letter to Media Educators*, MEDIA LITERACY REVIEW, 1993, http://wwinteract.uoregon.edu/MediaLit/mlr/readings/articles/goodman.html; Interview by Robert W. McChesney with Edward S. Herman,

Model Penal Code gave for not criminalizing defamation was the often-trivial nature of the material at issue.[195] They differentiated between "the ordinary case of defamation compensable in a civil suit" and gossip.[196] This distinction had both a substantive and a methodological component; that is, it was based both on the nature of the material being disseminated and the method used to disseminate it.[197]

The rationale for not criminalizing defamation was the product of three assumptions: (i) that if defamatory material were published, it would concern a public figure[198] (whose activities would be deemed a matter of general public interest) and would be published by an MSM entity from which the victim could obtain civil redress;[199] (ii) that the MSM would not publish defamatory material concerning non-public figures (because it would not be deemed a matter of general public interest); and (iii) that defamatory material not published by the MSM would be disseminated, if at all, parochially, by word of mouth (and limited print form).[200] The distinction the draft-

---

The Political Economy of the Mass Media, MONTHLY REVIEW, Jan. 1989, http://www.chomsky.info/ onchomsky/198901--.htm.

[195] *See supra* note 68 and accompanying text.

[196] *See supra* note 68 and accompanying text. "Gossip" has been defined as "casual conversation or unsubstantiated reports about other people." CONCISE OXFORD ENGLISH DICTIONARY 613 (11th ed. 2004). As this definition suggests, gossip has two characteristics: It is disseminated orally, on a very limited scale; and it involves "private" information. *See, e.g.*, Wikipedia, *Gossip (disambiguation)*, http://en.wikipedia.org/wiki/Gossip (gossip is defined as "news" that is spread "from person to person, especially rumors or private information"); Ronald de Sousa, *In Praise of Gossip: Indiscretion as a Saintly Virtue*, http://www.chass.utoronto.ca/ ~sousa/gossip.html (last visited Jan. 14, 2007) (gossip is "*conversation about other people's private lives*").

[197] *See supra* note 68 and accompanying text.

[198] A public figure would be either a public official or someone "who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention, are properly classified as public figures." Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974). The drafters of the Model Penal Code noted that most of the rare criminal libel prosecutions that had been brought over the past decade and a half involved public figures. *See* MODEL PENAL CODE § 250.7, cmt. at 44 n.6 (Tentative Draft No. 13, 1961).

[199] As noted earlier, the drafters of the Model Penal Code assumed civil liability would control the incidence of published defamation, as well as compensating its victims. *See supra* Part III.A.

[200] *See supra* notes 195, 199; *see, e.g.*, McIntyre v. Ohio Elections Com'n, 514

ers of the Model Penal Code drew between gossip and actionable defamation was therefore based more on the method that is used to disseminate defamatory material than on its content. They realized that publication by the MSM—the only type of publication then possible—vastly expands the scale on which defamatory material is disseminated and thereby increases the harm it causes;[201] to paraphrase Warren and Brandeis, what is whispered in the closet does far less damage than what is broadcast to the world.[202]

These assumptions that the drafters of the Model Penal Code made were valid when they decided not to criminalize defamation but, as is explained below, their validity has been eroded by the rise of online publication. Before we examine that issue, however, we need to resume our examination of how the traditional model of publication filters content.

The real-world model also applies a secondary filter: Once an item is selected for publication by an MSM entity, it undergoes a vetting that is intended to ensure the accuracy and fairness of the material to be published.[203] This process is dictated both by professional ethics and by a desire to avoid being held civilly liable for defaming those featured in the publication.[204] Although the drafters of the Model Penal Code did not

---

U.S. 334, 343-44 (1995) (leaflets); Talley v. California, 362 U.S. 60, 61 (1960) (handbills).

[201] *See, e.g.*, Ray v. Citizen-News Co., 57 P.2d 527, 528 (Cal. Ct. App. 1936). The terms harm and harms will be used to denote the very specific type of injury attributable to an activity that has been, or is sought to be, criminalized. *See, e.g.*, WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 1.2(e) (2d ed. 2003).

[202] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890), *available at* http://www.louisville.edu/library/law/brandeis/privacy.html ("'[W]hat is whispered in the closet shall be proclaimed from the house-tops'").

[203] *See* supra note 100; *see also* Wikipedia, *Journalism Ethics and Standards*, http://en.wikipedia.org/wiki/Journalism_ethics_and_standards (last visited Jan. 14, 2007). "Fairness" encompasses concerns such as minimizing intrusions into individuals' privacy and respecting victims' grief. *See id.* One ethical code, for example, notes that "private people have a greater right to control information about themselves than do public officials and others who seek power, influence or attention." Society of Professional Journalists, Code of Ethics, *supra* note 100.

[204] *See, e.g.*, Wikipedia, *Journalism Ethics and Standards*, *supra* note 203.

cite this process as a factor supporting their decision not to criminalize defamation, it no doubt played a part in that decision, as the vetting process also limits the frequency with which defamatory material is published by MSM.

MSM entities have the incentives and ability to filter content because they are part of a closed, hierarchical, commercial system—a modern guild.[205] MSM has historically been a closed, commercial system because of (i) the tremendous production costs involved in printing or broadcasting content and (ii) the need to control content so it is commercially viable and does not expose MSM entities to civil liability.[206] MSM entities are hierarchically-organized because hierarchical organization is the most effective way to orchestrate personnel and other resources for the accomplishment of tasks in the real, physical world.[207] All of this combines to create a finite operational context with shared understandings and standardized procedures.

As the incidents we examined in Part III(B) illustrate, online publication changes all of this. Cyberspace favors lateral, distributed organization rather than the hierarchical structures that prevail in the real-world; it also eliminates the financial and other barriers that make MSM a closed system.[208] In cyberspace, publication is egalitarian and "[m]ass amateurization" is the norm.[209] As one observer noted, while MSM creates audiences, online publishing creates communities, and communities do not filter content: "Writers submit their stories in advance, to be edited . . . before the public ever sees them. Participants in a community . . . say what they have to say, and the good is sorted from the mediocre after the fact."[210]

---

[205] *See, e.g.*, Wikipedia, *Guild*, http://en.wikipedia.org/wiki/Guild#Modern_guilds; *see also supra* note 193.

[206] *See, e.g.*, Douglas Gomery, *Media Ownership: Concepts & Principles*, *in* MEDIA ECONOMICS: THEORY AND PRACTICE 45-46 (Alison Alexander, et. al. eds., 1998). The need to limit civil liability is of less importance in this regard than ensuring content is commercially viable.

[207] *See, e.g.*, Brian Nichiporuk & Carl H. Builder, *Societal Implications*, *in* IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE 295, 297-301 (John Arquilla & David Ronfeldt eds., 1997); *see also supra* note 193.

[208] *See* Shirky, *Weblogs and the Mass Amateurization of Publishing*, *supra* note 191.

[209] *See id.*

The "amateur author/publisher" and "community" analogies accurately capture some aspects of online publication, but they miss others. Online publication does eliminate MSM's reliance on professional staff; as we saw in Part III(B), *anyone* who is literate and who has access to the Internet can create content[211] and publish it online,[212] directly or by using an intermediary. The "amateur" analogy captures that aspect of online publishing, but it can also imply that online authorship resembles MSM publishing in that the author of content is identifiable. That is, as we saw in Part III(B), not always true: Online authors can identify themselves (the activist who "outed" Edward Schrock),[213] can remain anonymous (the person(s) responsible for the Curzon-Brown postings)[214] or can pretend to be someone else (David Dabbert).[215]

The availability of all three alternatives—and particularly the last two—means that the online publishing model differs significantly from the real-world model upon which the drafters of the Model Penal Code relied. In the first alternative, we know who the author of the content is, but we may not know anything about that person; the less we know about the author of online content, the more difficult it is for us to assess the merits of what she says.[216] We (some of us, anyway) may therefore credit content that is distorted or completely fabricated.[217] This tendency is exacerbated when the author of the content remains anonymous or pretends to be someone else, someone with whom we believe we are communicating directly.[218]

---

[210] Clay Shirky, *Broadcast Institutions, Community Values*, Sept. 9, 2002, http://www.shirky.com/writings/broadcast_and_community.html.

[211] Our discussion of "publishing" content has tended to assume textual content, but it is not at all difficult to create and publish audio and/or visual content. *See supra* note 160.

[212] *See, e.g.*, Barrick Gold Corp. v. Lopehandia, [2004] 71 O.R.3d 416 (Can).

[213] *See supra* Part III.B.2.

[214] *See supra* Part III.B.3.

[215] *See supra* Part III.B.3.

[216] We have become accustomed to MSM entities, and so tend to assume that the information they provide is credible. This tendency is so deeply ingrained we may not be aware of it, except, perhaps, when we encounter colloquial expressions such as "newspaper of record." *See, e.g.*, Wikipedia, *Newspaper of Record*, http://en.wikipedia.org/wiki/Newspaper_of_record (last visited Jan. 14, 2007); *see also* Wikipedia, *The New York Times*, http://en.wikipedia.org/wiki/New_York_Times

Our relative or complete lack of knowledge as to the identity and bona fides of authors of online content differentiates it from content generated by real-world communities. Participants in a community not only know each other's identities, they also have (i) data that lets them assess the merits of what other community members say and (ii) shared experiential and emotional ties that keep their communications within certain, acceptable bounds. The first factor goes to the issue discussed above—our ability to assess the merits of what someone says. The second factor goes to a different issue: Community ties have historically acted to filter the content of communications in a fashion that is analogous to, but is less formal and probably less effective than, the standards and procedures used by MSM.[219]

This is where the "community" analogy for online publishing breaks down: While there *are* communities in cyberspace, and while these communities share ties that tend to maintain a level of civility in their mutual communications, this is not true of cyberspace itself. There are communities in cyberspace, but cyberspace itself is not a community; cyberspace is a frontier, a conceptual, unsettled, unstructured frontier.[220] As we have

---

(last visited Jan. 14, 2007).

[217] *See, e.g.*, *Barrick Gold Corp.*, 71 O.R.3d at 314 ("Internet defamation is distinguished from its less pervasive cousins, in terms of its potential to damage the reputation of individuals and corporations, by . . . its potential for being taken at face value").

[218] *See supra* Part III.B.3; *see also Barrick Gold Corp.*, 71 O.R.3d at 31 ("the anonymous nature of such communications may itself create a greater risk that the defamatory remarks are believed").

[219] Community ties are a particularly effective means of exerting informal social control. *See, e.g.*, Stephanie W. Greenberg & William M. Rohe, *Informal Social Control and Crime Prevention in Modern Urban Neighborhoods*, *in* URBAN NEIGHBORHOODS: RESEARCH AND POLICY 79, 81-94 (Ralph B. Taylor ed. 1986).

[220] *See, e.g.*, *That Wild, Wild Cyberspace Frontier*, RAND RESEARCH REVIEW, Fall, 1995, *available at* http://www.rand.org/publications/randreview/issues/RRR.fall

seen, it is easy to remain anonymous in cyberspace or to operate under a pseudonym (which may be a borrowed identity).[221] Many find this possibility intoxicating, and some exploit it to harm others by publishing problematic content (among other things).[222] Indeed, it seems that our ability to conceal our identities online encourages uncivil, antisocial behavior in the same way and for the same reasons that our operation of motor vehicles produces "road rage."[223] What this means for online publication is that it is constrained neither by the formal standards that govern MSM publication nor by the informal standards that structure behavior in the real, physical world.

Finally, online publication differs from traditional publishing in yet another way, a way the drafters of the Model Penal Code could not have imagined. Cyberspace not only democratizes publishing,[224] it accelerates it:

> Internet communications . . . are communicated through a medium more pervasive than print, and for this reason they have tremendous power to harm reputation. Once a message

---

95.cyber/wild.html ("Cyberspace, like the old West, is a lawless domain of limitless possibilities—for good but also for evil") (emphasis omitted).

[221] *See supra* Part III.B.3.

[222] *See supra* Part II.B; *see also* Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology and the Constitution*, 7 U. FLA. J. TECH. L. & POL'Y 123 (2002), *available at* http://grove.ufl.edu/~techlaw/vol7/issue2/brenner.pdf.

[223] *See, e.g.*, Susan W. Brenner, *Toward A Criminal Law for Cyberspace: Product Liability and Other Issues*, 8 U. PITT. J. TECH. L. & POL'Y 2 (2005) ("'Most of us have . . . observed that driving an automobile can alter a person's behaviour from civility to incivility'. . . . [O]ur visibility . . . is reduced when we operate a vehicle; [and that] erodes our sense of social responsibility. The same is true—but to an even greater extent—of our participation in cyberspace. . . . [I]n the cyberworld we can achieve complete anonymity and thereby divest ourselves of the . . . real-world and the behavioral constraints it imposes. This certainly does not mean that everyone who ventures into cyberspace . . . embarks upon . . . antisocial . . . acts. . . . It is, however, clear that people are taking advantage of the liberation they feel online to engage in behaviors they would never have felt free to indulge in the real-world.") (quoting M. E. Kabay, Address at the Annual Conference of the European Institute for Computer Anti-virus Research, *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, (Mar. 1998)) (footnotes omitted).

[224] *See supra* note 208-10 and accompanying text.

> enters cyberspace, millions of people worldwide can gain access to it. Even if the message is posted in a . . . forum frequented by only a handful of people, any one of them can republish the message by . . . forwarding it instantly to a different discussion forum. And if the message is sufficiently provocative, it may be republished again and again. The extraordinary capacity of the Internet to replicate almost endlessly any defamatory message lends credence to the notion that "the truth rarely catches up with a lie."[225]

This aspect of online publishing goes not only to its aggravated ability to inflict harm,[226] but also to the inefficacy of civil liability as both a remedial measure and a control mechanism.

The *"Star Wars* Kid" saga highlights its limitations as a remedial measure: The victim in that incident eventually sued the students who put his video online but they seem to have been, if not completely judgment-proof, unable to pay substantial damages.[227] And damages would do little to remediate the harm Raza suffered; his video is still online, where it will no doubt remain for years. The adolescents he sued may have disavowed their part in putting it online, but there is nothing they can do to erase the video from the Internet, and there is nothing a court can do, either. As the above-quoted passage notes, once it is put online, content "travels" around the world, ultimately remaining beyond the reach of courts in any particular jurisdiction.[228] As Raza learned, with online publishing it is remarkably difficult, if not impossible, to "put the cat back in the bag"—to un-do what has been done.[229]

His saga also highlights civil liability's limitations as a control mechanism. Raza could, and did, sue the classmates who initially put his video online, which *may* deter them from doing something similar in the future. He cannot, however, sue everyone who copied, modified and/or distributed his video once it arrived online. Real-world defamation suits can target one or a few defendants because real-world publication involves a single, simultaneous release of content by an MSM entity; online publication involves a repetitive series of cascading events, each initiated by a different person or persons, so the defendant pool is likely to be large and may be additive, *i.e.*, may continue to increase. Raza would have had to sue hundreds, if not thousands,[230] of people in various countries, most, if not all, of whom would be judgment-proof.[231] To obtain any redress,[232] Raza would have had to fund this gargantuan litigation himself,[233] which he could not do and which other victims of online defamation will no doubt find equally impossible. Online publishers understand these limitations, so the very-hypothetical prospect of civil liability does little, if anything, to control what they publish.

---

[225] Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 863-64 (2000) (quoting Gertz v. Robert Welch, Inc., 418 U.S. 323, 344 n.9 (1974)) (footnotes omitted).

[226] *See infra* Part IV.A.

[227] *See supra* Part III.B.1.

[228] *See generally* Oren Bigos, Note, *Jurisdiction Over Cross-Border Wrongs on the Internet*, 54 INT'L & COMP. L. Q. 585, 603 (2005).

[229] *See, e.g.,* Barrick Gold Corp. v. Lopehandia, [2004] 71 O.R.3d 416 (Can) (harm to corporation caused by online defamatory material).

Online publication clearly differs from the real-world model of publication that was the implicit empirical foundation of the decision not to include a provision criminalizing defamation in the Model Penal Code. It differs in ways that undermine, if they do not invalidate, the rationale responsible for that decision. That, however, does not *necessarily* mean we should criminalize defamation; the decision to criminalize an activity involves a complicated calculus, a balancing of principles and pragmatism. We undertake that task in the section immediately below.

---

[230] According to some estimates, the video—in its various incarnations—has been seen by as many as 15 million people. *See, e.g.*, Jerry Lawton, *Its' Daft Vader . . . But Star Wars Geek Has Last Laugh*, DAILY STAR (UK), Aug. 27, 2003, at News.

[231] And if it were undertaken, such an effort would also encounter the jurisdictional obstacles noted above. *See supra* note 228 and accompanying text.

[232] A victim might, for example, seek an injunction requiring the removal of the defamatory content from the Internet rather than damages for its having been distributed. *See generally* Complaint, Steinbuch v. Cutler, 2006 WL 3060084 (D. D.C. Oct. 30, 2006) (No. 05-0970(PLF)).

[233] Even if some/all of the defendants were not judgment-proof, most countries do not allow contingent-fee arrangements. *See, e.g.*, Ilana T. Buschkin, Note, *The Viability Of Class Action Lawsuits In A Globalized Economy—Permitting Foreign Claimants To Be Members Of Class Action Lawsuits In The U.S. Federal Courts*, 90 CORNELL L. REV. 1563, 1596 (2005). Since most or all of them are likely to be judgment-proof, a U.S. attorney would not be likely to take a case such as this on that basis.

IV. CRIMINAL DEFAMATION?

> *"The . . . aim of the criminal law is . . . to prevent injury to the health, safety, morals and welfare of the public."*[234]

As noted above, in deciding whether to criminalize an activity we must evaluate principle and pragmatic considerations. The drafters of the Model Penal Code did this in deciding *not* to criminalize defamation.[235] They considered the harm defamation then inflicted (principle) and the extent to which civil liability then sufficed as a control mechanism (pragmatism). In revisiting their decision, we are employing the same calculus, but in a different order. The section above addressed the pragmatic considerations, explaining how online publication erodes civil liability's effectiveness as a control mechanism; the pragmatic considerations that shaped the decision not to criminalize defamation are therefore far less compelling than when that decision was made. Part IV(A) examines the issue of harm, *i.e.*, whether online publication exacerbates the nature and severity of the harm attributable to defamation so that this harm now warrants the imposition of criminal sanctions. Part IV(B) offers a note on enforcement.

A. Harm

> *"Libel . . . is notoriously difficult of exact definition."*[236]

---

[234] LAFAVE, *supra* note 201, at § 1.2(e) (emphasis added).

[235] *See supra* note 61.

[236] State v. Weston, 501 S.W.2d 622, 623 (Ark. 1973) (emphasis added).

The basic component—the basic operational unit—of criminal law is a "crime." A crime (also known as an "offense") is conduct law makes punishable because it inflicts what has been determined to be a socially-intolerable type of harm.[237] There will therefore be a correlation between a crime and a specific harm. This correlation will be exclusive; that is, there will be one crime—and only one crime—for each proscribed harm.[238]

The drafters of the Model Penal Code recognized that real-world defamation inflicted harm, but did not think the harm warranted criminalization.[239] After explaining that harms are criminalized either because they are "very grave" or because of the "higher likelihood" that they will be inflicted, the architects of the Code decided defamation fell into neither category.[240] They inferentially, and correctly, concluded that it does not fall into the first category.[241] As to the second category, they concluded that while the traumatic harm caused by "certain aggravated" types of defamation might qualify for criminalization, the likelihood of such situations occurring (given the MSM's then-domination of publication) was too slight to justify making defamation a crime.[242] They also concluded, by implication, that the far more likely but less traumatic harm caused by routine defamation (gossip) did not justify criminalization; this conclusion seems to have been based on the very limited scale upon which this residual class of defamatory material could be disseminated in a pre-Internet era.[243]

Things have changed.[244] The aggravated and routine varieties of defamation—along with some new variants—have migrated online where, it is clear, they will thrive and proliferate absent the introduction of control mechanisms more effective than conventional civil liability.[245] Does this alteration in the empirical context the drafters of the Model Penal Code assumed, and relied on, justify rejecting their decision and embarking upon the criminalization of defamation?

---

[237] *See* BLACK'S LAW DICTIONARY 399 (8th ed. 2004) (definition of "crime"). For more on this, see Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 11.

[238] *See generally* MODEL PENAL CODE § 1.07(1) (1962).

[239] *See supra* Part II.C.

[240] *See supra* Part II.C.

[241] *See supra* Part II.C.

[242] *See supra* Part II.C; *see also* Part III.C.

[243] *See supra* Part II.C; *see also* Part III.C.

[244] *See supra* Part III.

It is difficult to answer that question. Online publication has not only made problematic speech—speech that may or may not qualify as defamation[246]—more common, it has made it more complex. When the Model Penal Code was written, defamation was for the most part an established, predictable phenomenon that consisted of an MSM entity's publishing text, photographs or, on occasion, video.[247] The resulting harms were consequently stable: the published material "blackened" the victim's reputation and/or held her up to public ridicule.[248]

The section above explained how and why online publication changes the unitary nature of traditional, MSM publishing.[249] While our experience with online publication is in its infancy, it is already apparent it introduces a substantial "wild card" element into the process.[250] Anyone with access to the Internet can publish whatever he or she wishes in any of several formats: "real" or altered text, photographs, video and/or audio. The section above explained why this change in the nature of publishing requires that we reconsider the Model Penal Code drafters' decision not to criminalize defamation;[251] to do that, we must assess the harms inflicted by the twenty-first century version of defamation. There would, after all, be no reason to employ penal sanctions in this context if the harms being inflicted are comparable to those with which the drafters of the Model Penal Code were familiar.

---

[245] *See supra* Part III.C. Online defamation will persist and perhaps increase in incidence and virulence for at least two reasons: One is that cyberspace lets us broadcast the gossip, vituperation and otherwise-malevolent communications that have always played some part in human society; the other reason is that cyberspace empowers our antisocial tendencies in the same way as, and for the same reasons as, our operation of motor vehicles. *See supra* Part III.C. Online defamation will only be further exacerbated as communication technologies increase in sophistication and in pervasiveness. *See generally* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667 (2006).

It is at least theoretically possible that a modified version of conventional civil liability could be used to control online defamation along with, or instead of, criminal liability. How (and if) that could be done is quite outside the scope of this article, however.

[246] *See supra* Part III.B.

[247] An unscientific search of *Westlaw* for state civil and criminal defamation cases decided between 1946 and 1961 shows that nearly all of them arose from text and/or photographs published in newspapers or magazines; a few involved motion pictures.

[248] *See supra* Part II.A. The *Restatement* and other, traditional formulations of defamation link reputational injury and being held up to ridicule. *See* Part II.A. The analysis presented below treats these as separate and distinct harms, on the premise that this more accurately reflects modern conceptualization of defamation as encompassing both reputational injury and emotional, or psychic injury. *See* RODNEY A. SMOLLA, LAW OF DEFAMATION § 1:24 (2d ed. 2006). The impetus for dichotomizing what was once regarded as a unitary harm comes from modern publishing techniques, which can result in the dissemination of material that ridicules without impacting upon one's reputation. *See infra* Part IV.A.1-2.

The first two sections below, therefore, undertake the rather daunting task of parsing the harms currently inflicted by the online publication of problematic speech.[252] It is a daunting task because the pliancy of online media creates almost unbounded opportunities for producing and publishing problematic speech. Some of this speech will clearly inflict harms equivalent to or greater than those traditionally associated with defamation, but some will not; and some of it will be problematic, injurious speech the equivocality of which challenges our ability to classify it as harmful or not-harmful. Since it is impossible, here, to explore all of the harms that can be inflicted by online publication, the analysis presented in the first two sections is illustrative, not exhaustive. It focuses on a threshold issue: Does online publication inflict harms that justify the use of penal sanctions to control online defamation? Since we are exploring the fit between the harms traditionally associated with real-world defamation and the new harms attributed to online defamation, the sections use the traditional harms (reputational injury and ridicule) as baseline, or organizing, principles.[253] The third section then assesses the need to criminalize defamation in light of the preceding analyses.

---

[249] *See supra* Part III.C.

[250] *See supra* Part III.

[251] *See supra* Part III.C.

[252] The rapidly evolving nature of modern communications technology means we will have to revisit these issues periodically, as new technologies further expand opportunities to disseminate problematic speech.

1. Reputation

> *"Among the rights . . . the law undertakes to protect, that of reputation is one of the most prominent."*[254]

The harm defamation inflicts upon reputation is primarily relational.[255] As one source notes, defamation law is concerned with "disruption of the 'relational interest' that an individual has in maintaining personal esteem in the eyes of others."[256] This "relational interest" has three components: (i) existing relations with others; (ii) prospective relations with others; and (iii) an existing "public image" or the ability not to acquire a negative "public image."[257]

While both are amorphous, reputational harm is the more concrete of the two types of harm traditionally associated with defamation. Unlike ridicule, which can be more nuanced,[258] reputational injury tends to be less subject to disputation because the harm tends to be more immediately outrageous, more "in your face." The false light cases outlined above are a good example of this;[259] in each instance, someone published material online that attributed socially-unacceptable traits, desires and/or behaviors to the victim(s). Depending on the particular case, the material was such that it would undermine the individual's personal relations with others and could negatively impact professional relationships.[260] To the extent that family, friends, colleagues or acquaintances credited the allegations against these individuals, each suffered a loss of reputational capital; the image—the "face" each presents to the world—was debased.[261] And if educators can be deemed to have (or aspire to have) a public image, then the postings directed at Curzon-Brown and Wagner presumably inflicted similar damage on this aspect of their relational interests.[262]

---

[253] *See supra* note 248.

[254] Knickerbocker Life Ins. Co. v. Ecclesine, 6 Abb. Pr. (n.s.) 9 (N.Y. Sup. Ct. 1869) (quoting Justice Clerke's jury charge) (emphasis added).

[255] *See, e.g.*, SMOLLA, *supra* note 248, at § 1:22. Dean Smolla suggests that reputational assaults also inflict economic and emotional harms, but it seems that these interests are, in most cases, encompassed by the harm to one's relational interests. *See id.* at §§ 1.23-.24.

[256] *Id.* at § 1:22.

[257] *See id.* (citing David A. Anderson, *Reputation, Compensation and Proof*, 25 WM. & MARY L. REV. 747, 764-66 (1984)).

[258] *See infra* Part IV.A.2.

[259] *See supra* Part III.B.3.

The harm inflicted in the false light cases is readily apparent because each involved the online publication of information that was clearly, demonstrably false. The truth or falsity of published material was traditionally irrelevant in imposing criminal liability for defamation; since the gravamen of the common law crime was distributing content that could cause a breach of the peace, accuracy was immaterial.[263] But accuracy—or, more precisely, inaccuracy—is very material to calculating harm. While metrics have never been devised for defamatory harms, it is reasonable to infer that the publication of derogatory *false* information will have a significant deleterious impact on one's reputation among those with whom the individual maintains and/or aspires to maintain relationships. Because the information is false, it inflicts reputational harms that would otherwise not have arisen; since, for example, David Dabbert's former boss was not really interested in "sex on the side," information to that effect would never have circulated in her community and tarnished her reputation but for his putting a false claim to that effect online.[264]

The Dabbert case also shows how online publication can aggravate defamatory harms. First, assume the basic facts:

---

[260] *See supra* Part III.B.3.

[261] *See, e.g.*, Debra J. Saunders, *Right to Flame Can't Make It Right to Flame*, S.F. CHRON., May 2, 2000, *available at* http://www.sfgate.com/cgi bin/article.cgi?file=/chronicle/archive/2000/05/02/ED41804.DTL ("'People can send in multiple reviews of you and destroy your reputation.'") (quoting Daniel Curzon-Brown).

[262] *See id.*

[263] *See supra* Part II.A-B.

[264] *See supra* Part III.B.3.

Dabbert's boss fires him, which makes him so angry he decides to "strike back" by accusing her of behavior her community will find extremely disreputable. Now assume this occurred forty years ago, before the Internet. How could Dabbert disseminate his accusations? Since no MSM entity would publish such unfounded allegations, he would have to rely on word of mouth, initiating a whispering campaign to spread the rumor that his former boss sought "sex on the side" (however one did that in a pre-Internet world). Those who heard the rumor from Dabbert would know it came from one with a grudge against the woman, and would assess it in that light; those who heard it indirectly and had no way of knowing who it came from would probably not be inclined to give much weight to an unattributed, implausible rumor about a (presumably) respected member of the community. This gossip scenario is what the drafters of the Model Penal Code had in mind when they decided not to criminalize defamation because of the very limited harm it inflicted.[265]

Now consider the twenty-first century version of the scenario: Instead of relying on an *ad hoc* whispering campaign that might ultimately be traced to him, Dabbert goes online, poses as his former boss (using her personal information to provide credibility) and posts a message saying "she" seeks "sex on the side." His revenge apparently lay in knowing she would receive responses to "her" inquiry that would frighten and embarrass her; he could have compounded the reputational injury to this woman if he had anonymously sent the posting to her boss, her minister, the principal of her children's school, etc. In either event, Dabbert inflicts a significantly greater level of reputational harm on his victim than in the gossip scenario because here it seems that this is no rumor; it seems this is truly something the victim herself has done. Online publication not only gives people like Dabbert the ability to broadcast defamatory material, it also lets them engage in imposture—using the victim's own persona to defame her.[266]

---

[265] *See supra* Part II.C.

[266] In some states, anyway, this aspect of Dabbert's conduct might constitute

The "Holla Back NYC" and "Don't Date Him Girl" examples show how online publication can harm someone's reputation in intermediate cases, *i.e.*, when the truth of the material being disseminated is subject to dispute. The material posted on these sites comes from motivated individuals who offer their interpretations of their experiences (street encounters for "Holla Back," dates for "Don't Date Him Girl") with anonymous or identified men.[267] Since both sites encourage venting, the postings are almost exclusively negative; many of them are quite inflammatory (for different reasons). Both sites identify the subjects of the postings, though in varying ways and varying degrees: Those who post on "Don't Date Him Girl" know the man they are warning others about and therefore include varying amounts of personal information about him; since those who post on "Holla Back" are reporting street encounters, they generally do not know names and so rely on photographs or physical details to identify the men they cite for misconduct.

While the truth or falsity of published information is irrelevant in imposing criminal liability for defamation, accuracy is, as noted earlier, of empirical significance in assessing harm. The allegations that appear on the "Holla Back" and "Don't Date Him Girl" websites are not filtered or verified in any way; they come from individuals who are agitated as a result of an experience they have had with a man or men. Impostors like Dabbert could use these sites for malicious ends,[268] but since we have addressed that scenario we will assume for the purposes of this analysis that the postings are at base legitimate, *i.e.*, that they come from someone who really had an encounter (i) of the type at issue in the posting (ii) with the individual(s) identified in the posting. Given that assumption, then, do postings on sites like "Holla Back" and "Don't Date Him Girl" inflict harms—the generic severity of which warrants the imposition of criminal liability for publishing defamatory material?

---

criminal impersonation. *See, e.g.*, ALA. CODE § 13A-9-18 (1975); CONN. GEN. STAT. ANN. § 53a-130(a) (1971); NEB. REV. STAT. § 28-608(1)(a) (1977).

[267] *See supra* Part III.B.4.

[268] *See supra* note 189.

Or do they merely represent the migration of gossip online?

Those are difficult questions. No one, presumably, would argue that being vilified on a website like this inflicts harm equivalent to that resulting from rape or murder.[269] But what about the residual category the drafters of the Model Penal Code cited—an increased likelihood of lesser harms analogous to those resulting from "petty theft or malicious mischief?"[270]

The opportunity websites such as these provide for "outing" men who allegedly engaged in boorish (if not criminal) behavior dramatically increases the likelihood that what the men thought was private will become a public anecdote. If that occurs, it at least arguably produces two distinct but related harms: (i) a loss of control over one's private activities; and (ii) having an idiosyncratic view of one's private activities broadcast to the public. The potential for inflicting either or both harms might warrant the imposition of criminal liability for defamation, depending on (i) the likelihood that harm will be inflicted and (ii) the nature and severity of the resulting injury to the victim.

As to the first issue, we are concerned not with a quantitative assessment of the relative frequency with which individuals are likely to find their private lives becoming an anecdote on a website versus the frequency with which they are likely to become the victims of "petty theft or malicious mischief." The drafters of the Model Penal Code cited these crimes as examples of lesser harm-inflicting behaviors, the incidence of which is not so remote that it is unnecessary and inadvisable to use criminal liability to control them.[271] Writing in an era when publication was controlled by MSM entities, they assumed the publication of gossip or other calumnies was too remote to make this necessary and advisable. That assumption no longer holds.[272] The sections below therefore consider whether the nature and severity of either/both of the harms identified above make it necessary and advisable to use criminal liability to discourage their infliction.

---

[269] *See supra* Part II.C.
[270] *See supra* Part II.C.
[271] *See supra* Part II.C.
[272] *See supra* Part III.C.

We begin our analysis with the second harm, because it is a purely defamatory harm. The first harm encompasses compromising someone's privacy as much as it does using allegedly private information to damage their reputation; since it implicates privacy concerns as well as defamation, we defer our consideration of this harm until we finish our examination of purely defamatory reputational harms.[273]

a. Reputational Harm

The second harm identified above can inflict reputational injury that is at least equivalent to the financial injury caused by petty theft and/or malicious mischief. To illustrate the nature and effect of this harm, we will consider two scenarios, one for each website.

i. "Holla Back"

John Doe, an associate in a New York City law firm, learns that a cell-phone photograph of him riding to work on a city bus has been posted on the "Holla Back" website along with the allegation that he was exposing himself to women on the bus. Doe learns this from a person (associate, paralegal, executive assistant) in his office, who says it has become a matter of common knowledge in the office. He begins to receive emails and calls from colleagues outside his office, from his family, from the woman he has been dating, from friends and so on. All of them have heard about the posting; most have seen it.

The posting will have a dramatic, negative effect on Doe's professional and personal reputation; he has been publicly identified as a pervert, a criminal.[274] This is true even though we are assuming that the allegation is false and that the photograph merely shows Doe seated on a city bus. If the allegation is false, this scenario is analogous to—though more egregious than—the Dabbert scenario analyzed above. It is analogous in that by publishing a false accusation (along with Doe's photograph), his anonymous accuser has tainted a much, much wider audience than she could have reached with oral gossip. It is somewhat more egregious because the fact that the accusation is published on a site which "outs" behavior such as that being attributed to Doe and is accompanied by a photograph of Doe on a city bus inferentially enhances the presumptive credibility of what is in fact a falsehood.[275]

---

[273] *See infra* Part IV.A.1.b.

[274] *See* N.Y. PENAL LAW § 245.01 (McKinney 2005).

If the accusation is false, why would someone post it? We are assuming postings on this site are made in good faith, but we do not assume accuracy: Maybe the poster misunderstood something she saw; maybe she mistook Doe for someone else; maybe she is deranged. Who knows? When content is not filtered, errors will occur and harm will result.

What can Doe do to remediate the harm he has suffered? These sites seem loath to edit or remove postings,[276] so that is not a viable option. And as we saw earlier, civil liability offers Doe no recourse; the site is immune from suit and the poster is anonymous (and probably judgment-proof, as well).[277] It seems Doe has no recourse; he cannot publish a rebuttal, "unpublish" the accusation, or obtain vindication in a civil suit.

ii. "Don't Date Him Girl"

Assume John Doe is, once again, an associate in a New York City law firm. Assume he dated an associate from another firm, Mary Smith, for six months before they broke up three months ago. Doe started dating Jane Brown, a professor who knows Mary Smith, two weeks ago; yesterday he received an email from Jane that contained the message, "This really opened my eyes. Don't call me again!" and a link to the "Don't

---

[275] The nature of the site Dabbert used presumably enhanced the credibility of his falsehood, as well; the inclusion of the photograph of Doe, however, markedly increases the likelihood that those who see this accusation will credit it, to some extent, because people will tend to infer guilt from the unambiguous evidence of Doe's being on the bus.

[276] *See supra* Part III.B.4.

[277] *See supra* Part III.C.

Date Him Girl" website.

Doe clicked on the link and was shocked to find that someone (whom he now believes to be Mary Smith) posted an "Alleged Cheater" profile on "Don't Date Him Girl" using his name and photograph. The profile gives Doe's age, height, weight, eye and hair color, and correct place of employment, and it then embarks on a lengthy diatribe which, among other things, accuses him of being "a degenerate lothario," a "compulsive liar" and a "deadbeat" who "has a serious juvenile record."[278] The authoress of the post says Doe "cheated on" her with "MEN AND WOMEN," including her friends.[279] She accuses him of being a "Jekyll-Hyde" who "kept the ugly side of himself hidden" until the day he "abandoned" her for "my best friend."[280]

Doe is appalled. As far as he is concerned, the allegations are completely false; he calls Jane to tell her this, but she refuses to talk to him; she seems to believe what the profile says. Doe assumes Mary sent the profile to Jane but wonders how many other people have seen it. He calls and emails Mary, but she ignores him. He contacts "Don't Date Him Girl" and learns that while they will not remove his profile, he can post a rebuttal. Doe is not sure he should do this, since he would have to admit that he dated Jane, a friend of Mary's, and that he was charged with shoplifting when he was fourteen (the result, he says, of a "misunderstanding"). He could generally deny the profile's other allegations, but is afraid this would only lend them credence (and maybe prompt the author to post a surrebuttal). He hopes people at his law firm do not learn about the profile, as that would be embarrassing.

Doe suffers some harm to his reputation in this scenario, but it differs in several ways from the harm inflicted in the "Holla Back" scenario. For one thing, here he knows (or thinks he knows) who his accuser is; even if Mary Smith is not his accuser, the author of the posting must be a woman Doe dated at some point.[281] This puts the accusations into a familiar context: bad feelings between former lovers. Everyone is familiar with that context and so will be inclined to take the allegations in the profile with a grain of salt; this minimizes the reputational harm they will inflict.

---

[278] These allegations and those that follow are based on a "Don't Date Him Girl" profile of a Virginia man. DontDateHimGirl.com, http://dontdatehimgirl.com/search/ (last visited Jan. 14, 2007).

[279] *Id.* ("He'll try to seduce your friends (he did mine and used me as a decoy to draw in other women).").

[280] *See id.*

The allegations in the "Don't Date Him Girl" profile are also much less damaging than the accusation on the "Holla Back" site. While the "Holla Back" accusation imputed criminal behavior that is regarded as particularly opprobrious to Doe, the "Don't Date Him Girl" profile basically casts him as a cad (a deadbeat, lying lothario) with a "juvenile record." This latter allegation is unlikely to have much impact because the profile notes he is an attorney; most of those who see it will probably realize that he would not be practicing law if he really had a "serious" juvenile record. The remaining, obscure allegations (being a "Jekyll-Hyde," having an "ugly side" and cheating with MEN as well as with WOMEN) are also unlikely to carry much weight, if only because they are so vague and generalized.

Essentially, what we have here is the migration of gossip online. It differs somewhat from offline gossip in that it has been reduced to written form and published on a website that outs cads and cheaters; these circumstances mean the allegations will circulate more widely than if the author relied on oral transmission (rumor) and may acquire a certain cachet, a gloss of credibility, from being on a website (though there is an argument to the contrary).[282] Overall, though, it seems this scenario actually inflicts less harm than real-world gossip because Doe can post a rebuttal, which will appear whenever anyone accesses his profile.

---

[281] We are assuming the posting is legitimate, *i.e.*, was posted by someone who dated Doe, and does not represent a Dabbert scenario. *See supra* notes 129-33.

[282] The argument is that this site exists to let women "vent" about men they have dated, which suggests that the allegations it publishes are more likely to be the product of emotion than accurate reportage. It is a variant of the "grain of salt" caveat noted earlier.

iii. Reputational Harm: Assessment

As the analysis in the preceding sections should illustrate, assessing the nature and severity of the reputational harm inflicted by online publication is a very complicated task. As the analysis in the immediately preceding two sections may demonstrate, much will depend on the nature of the website on which the information is published; what might seem to be blatantly specious allegations ("trades sex for grades") could harm a teacher's professional reputation if they were posted on a site like Teacher Review.[283] Another important factor is the accuracy of what is posted; we have already noted how posting false allegations can harm someone.[284] In the two sections immediately below we consider whether harm—more precisely, harm that is within the ambit of this analysis—results from the online publication of accurate information.

b. Privacy Harm

Although this is an article about defamation, we cannot ignore the issue of privacy. Privacy claims can arise in many contexts: The Foxy Felon postings; Cutler's publicizing her trysts with Steinbuch; the (apparent) "outing" of Congressman Schrock; and postings on sites like "Don't Date Him Girl" and "Holla Back" are all instances in which privacy was, or could have been, raised.[285]

People invoke privacy when an online publication involves the public dissemination of what they contend is private information.[286] Privacy also becomes an issue when—and only when—the information disseminated is true; one cannot, after all, claim a privacy interest in fictive activity.

Violating someone's privacy (actual privacy, as opposed to the aspirational privacy that usually surfaces in online publication cases)[287] is a serious matter. So serious that the drafters of the Model Penal Code included a provision criminalizing invasion of privacy in the final draft of the Code; the provision targets real-world invasions of privacy, which are not implicated in this analysis.[288] Actually, invasions of privacy generally are not implicated in this analysis.[289]

---

[283] *See supra* Part III.B.3.

[284] *See supra* Part IV.A.1.a.i.

[285] *See supra* Part IV.A.1.

[286] *See supra* Part IV.A.1.

[287] *See infra* notes 292-94 and accompanying text.

The privacy claims that surface in online publication cases are not *invasion* of privacy claims; they go, instead, to the act of publishing what the "victim" claims is—or should be—private information. We saw this in Part III(B), and again in Part IV(A)(1)(a). The Foxy Felon complained because official, public information about her criminal conviction was put online; Steinbuch, Schrock and the subjects of various postings on "Don't Date Him Girl" and "Holla Back" complained because information about their private activities in public places was put online.[290] This is the issue we noted earlier,[291] and deferred for consideration until now.

The first problem with these complaints is that the information at issue was not private because it concerned an activity the complainant conducted in conjunction with or in the presence of another person or other persons.[292] Activities are not private when we conduct them with or among others;[293] when we share our thoughts, our acts, our selves with others we assume the risk they will divulge what they have learned.[294] What you do in public—on a bus, on a street, in your lover's apartment, on a website, etc.—*is* public. It cannot be deemed private simply because it is discreditable or embarrassing; arguments to that effect mix metaphors, confuse principles, and impermissibly conflate privacy with defamation.

---

[288] *See supra* note 121.

[289] Traditional intrusions such as voyeurism, eavesdropping and compromising the privacy of the mail have long been criminalized. *See supra* note 121; *see also* 18 U.S.C § 1708 (2000) (listing the penalty for various criminal acts linked to stealing mail); H. Morley Swingle & Keviin M. Zoellner, *Criminalizing Invasion of Privacy: Taking a Big Stick to Peeping Toms*, 52 J. MO. B. 345, 345-59 (1996) (discussing Missouri criminal penalties for invasion of privacy). The same is true for more egregious intrusions, such as breaking into repositories containing private data or documents. *See, e.g.*, 18 U.S. Code § 1030(a) (2000) (criminalizing fraud in connection with activity related to computers); MODEL PENAL CODE § 221.1 (1962) (defining burglary).

[290] *See supra* Part III.B.2, 4.

[291] *See supra* Part IV.A.1.

[292] *See supra* Part III.B. This circumstance will be a constant in most online defamation claims. Defamatory publication circulates accounts of (allegedly) "discreditable" events. Online (or offline) publications learn about these events from observers with first-hand information; it is these observers who are the "source" of the defamatory material being published. One is, by definition, "defamed" by another, not by oneself. If the victim voluntarily shared the information at issue with the source, then the information was not private and the only act the victim can complain of is the act of publishing the material. If the act of publishing the

The other problem with these complaints goes not to the issue of privacy but to the issue of defamation. As was noted earlier, when victims of online publication invoke privacy, they are necessarily complaining about the dissemination of true information. The dissemination of true information can, of course, inflict reputational harm. Assume, for example, that the minister of a conservative Baptist church frequents strip clubs. Assume, further, that someone "outs" his predilection on a website, by posting digital photographs that show the minister at the strip club enjoying the performances. The online publication of this true information will inflict what may be devastating harm on his reputation.[295] But there is no necessary equivalence between the infliction of reputational harm and defamation.

Since civil defamation law is predicated on the need to redress harm to an individual, it has never encompassed the dissemination of true information.[296] As Blackstone observed,

---

material constituted defamation, then it provides the basis for the imposition of civil and/or criminal liability. Conversely, if the source of the information obtained it without the victim's knowledge by violating a legally-cognizable expectation of privacy, then its acquisition could constitute invasion of privacy and could support the imposition of civil and/or criminal liability on that basis. *See supra* note 121.

[293] The *Oxford English Dictionary*, for example, defines "private" as "not to be shared or revealed." CONCISE OXFORD ENGLISH DICTIONARY 1142 (11th ed. 2004). *See also* RESTATEMENT (SECOND) OF TORTS §§ 652A(2)(a), 652B (1977) (privacy as seclusion).

[294] *See, e.g.*, Lopez v. United States, 373 U.S. 427, 449-50 (1963) (Brennan, J., dissenting).

[295] *See generally* Trisha L. Howard, *Minister Accused of Solicitation Steps Down*, ST. LOUIS POST-DISPATCH, Dec. 5, 2003, at B1 (discussing a pastor's resignation after being arrested for solicitation of a prostitute).

[296] *See supra* Part II.C.

"if the fact be true, it is *damnum absque injuria*; and where there is no injury, the law gives no remedy."[297] Criminal defamation law, on the other hand, was historically predicated on the need to maintain social order by preventing breaches of the peace.[298] It therefore—at least originally— did not recognize truth as a defense, on the premise that "[t]he publication of matter which is true, may have quite as great a tendency to excite to breaches of the peace, as if false."[299]

The *Garrison* Court concluded that the common law breach of the peace justification for criminalizing defamation was not valid in the twentieth century,[300] a conclusion that presumably applies with equal force in the twenty-first century. The only remaining justification, therefore, for criminalizing defamation is the civil law premise: the publication of "*untrue*" information that defames someone and inflicts harm that the law must address.[301] Under the civil standard, publishing *true* information about someone may constitute a tortious invasion of privacy (or some other actionable transgression),[302] but it cannot constitute defamation.[303] The same rule should apply, for the same reasons, in the criminal context; we return to this issue in Part IV(A)(3).

---

[297] WILLIAM BLACKSTONE, 3 COMMENTARIES *125.

[298] *See supra* Part II.C.

[299] State v. Burnham, 9 N.H. 34 (N.H. 1837); *see also supra* note 52 and accompanying text.

[300] *See supra* note 82 and accompanying text.

[301] *See supra* Parts II.A., IV.A.1; *cf. infra* Part IV.A.2 (discussing ancillary effects of defamation).

[302] *See supra* note 121. Depending on the circumstances involved, the publication might constitute the intentional infliction of emotional distress, harassment or stalking. *See, e.g.*, 18 PA. CONS. STAT. ANN. § 2709 (West 2000 & Supp. 2005); WASH. REV. CODE ANN. § 9.61.260 (West Supp. 2005); RESTATEMENT (SECOND) OF TORTS § 46 (1977). This brings us back to the issue noted earlier: the premise that online speech is problematic in various ways. *See supra* Part III.B; *see also infra* Part IV.A.3.

[303] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS §§ 558 & 581A (1977). As noted earlier, the Supreme Court has suggested—but not held—that publishing true information concerning purely private matters may be protected by the First Amendment. *See supra* note 80.

2. Ridicule

> *"exposed her to the ridicule . . . of all who heard such language"*[304]

We are using ridicule—a term often found in defamation statutes[305]—as a residual category of harm. Although the publication of defamatory material primarily tends to harm the victim's reputation,[306] it can also have a secondary effect. Publishing defamatory material can harm our relationship with our self as well as our relationships with others; it can damage the self-esteem we derive from our internalized self-image.[307]

We saw two clear examples of this type of harm earlier. One was the mortification Kim Hyo-bi experienced when someone put distorted photographs of her online.[308] While people she knew saw them, the photographs would not cause Hyo-bi reputational harm because they in no way attributed negative acts or discreditable attributes to her. They made her look "silly,"[309] a circumstance others would probably comment on, but which would not alter their assessment of, or relationship with, Hyo-bi.[310] Logically, then, she suffered no harm; affectively, however, she was harmed because she *was* ridiculed,[311] both by the photographs themselves and by the fact that someone had done this to her. (The limited information available about this incident does not indicate that the publication of the photos caused Hyo-bi to suffer ridicule from others.)

---

[304] Stevenson v. John J. Grier Hotel Co., 251 S.W.355, 355 (Ark. 1923) (emphasis added).

[305] *See supra* note 18 and accompanying text.

[306] *See supra* Part IV.A.1.

[307] *See, e.g.*, R.A. STEFFENHAGEN & JEFF D. BURNS, THE SOCIAL DYNAMICS OF SELF-ESTEEM: THEORY TO THERAPY 28 (1987) (defining self-esteem as "the totality of the individual's constructs of self: self-concept (mental), self-image (physical), and social concept (cultural)"); *see also id.* at 19-30 (analyzing self-esteem).

[308] *See supra* Part III.B.1.

[309] "Silly" is a synonym for "ridiculous." *See, e.g.*, J.I. RODALE, THE SYNONYM FINDER 1040 (Warner Books ed., Warner 1986) (1978).

[310] No one would "believe" the distorted photographs: Acquaintances would know the pictures did not accurately depict Hyo-bi; and given the nature of the distortion involved, it seems reasonable to infer that anyone who saw them would realize this.

[311] *See, e.g.,* THE CHAMBERS DICTIONARY 1303 (9th ed. 2003) (defining "ridicule" as "to make fun of; to deride; to mock").

The other ridicule case is the "*Star Wars Kid*" saga. As a reporter noted, Ghyslain Raza became "a worldwide object of ridicule when schoolmates put on the Internet a video of him clumsily pretending to be a *Star Wars* character."[312] Unlike the morphed photographs of Hyo-bi, the video accurately depicted Raza voluntarily engaging in activity; here the ridicule derived not from a distortion of his image, but from the dissemination of a video many found amusing, given his earnest ineptitude as a Jedi Master.[313] Raza was humiliated by their amusement because it made him see his performance (his self) as they saw it: as ridiculous. As with Hyo-bi, nothing in the video damaged Raza's reputation; his documented ineptitude with a light saber would not cause others to refuse to associate with him.[314] Like Hyo-bi, therefore, Raza sustained the mere harm of ridicule (though the actual magnitude of the harm he sustained was much greater due to the wider, and more persistent, distribution of his video).

As these cases illustrate, ridicule produces psychic harm that is analogous to, but less severe than, the harm caused by intentionally inflicting emotional distress in violation of civil or criminal law.[315] Until the last century, criminal law was only concerned with physical harms; but over the last several decades scholars and legislators have accepted the premise that psychic harms unaccompanied by physical injury *can* warrant the imposition of criminal liability.[316] But not *every* psychic harm does warrant the imposition of such liability. As the authors of the *Restatement of Torts* explained, law cannot take cognizance of

---

[312] Ha, *supra* note 106.

[313] *See, e.g.*, *Star Wars Kid*, *supra* note 116. Unlike Hyo-bi, Raza was the object of ridicule by others, particularly his classmates. *See supra* Part III.B.1.

[314] Indeed, it generated some sympathy: At least 83,000 people signed a petition to have him given a role in the then-upcoming *Star Wars* movie. *See Star Wars Fans Seek Film Role for Internet Kid*, BBC NEWS, Sept. 5, 2003, http://news.bbc.co.uk/cbbcnews/hi/tv_film/newsid_3083000/3083122.stm.

[315] *See, e.g.*, MICH. COMP. LAWS ANN. § 750.411h(1)(b) (West 2004) (defining "emotional distress" under stalking law as "significant mental suffering or distress that may, but does not necessarily, require medical or other professional treatment or counseling"); *see also* RESTATEMENT (SECOND) OF TORTS § 46 cmt. j (1965) (discussing severe emotional distress). This type of harm was no doubt implicated in Steinbuch's suit against Cutler; *see supra* Part III.B.2.

> [I]nsults, indignities, . . . petty oppressions, or other trivialities. . . . [We] must . . . be hardened to a certain amount of rough language, and to occasional acts that are . . . unkind. There is no occasion for the law to intervene in every case where some one's feelings are hurt. There must still be freedom to express an unflattering opinion, and some safety valve must be left through which irascible tempers may blow off relatively harmless steam.[317]

Though the authors of the *Restatement* were explaining their decision not to impose civil liability for routine instances in which one person's actions cause another to suffer emotional distress, their rationale applies with equal force to online ridicule, as is explained below.

3. Sum

"Society has a pervasive and strong interest in preventing and redressing attacks upon reputation."[318]

Ridicule is not pleasant, but it does not have the ramifications associated with serious reputational harm. As we saw above, online resources can be used to disseminate material that will have a devastating effect on someone's reputation and, consequently, on his or her life. We used postings on the "Holla Back" site to illustrate this, but that is one, rather modest example. In the preceding section, we used a hypothetical about a conservative Baptist minister who likes strip clubs to illustrate why privacy is not a harm within the compass of this analysis. Let us now use that hypothetical for a different purpose—to illustrate more devastating ways in which online publication can be used to damage, or even destroy, someone's reputation.

---

[316] *See, e.g.*, Walter Block, *Berman on Blackmail: Taking Motives Fervently*, 3 FLA. ST. U. BUS. REV. 57, 87 (2002-03) *available at* http://www.law.fsu.edu/current_students/organizations/businessreview/vol3/block.pdf; Kimberly Wingteung Seto, Note, *How Should Legislation Deal with Children as the Victims and Perpetrators of Cyberstalking?*, 9 CARDOZO WOMEN'S L.J. 67, 85 (2002).

[317] RESTATEMENT (SECOND) OF TORTS § 46 cmt. d (1965).

[318] Rosenblatt v. Baer, 383 U.S. 75, 86 (1966) (emphasis added).

Assume the following: John Doe is the minister of a conservative Baptist church in Ada, Oklahoma; he has never visited a strip club and, indeed, strongly believes strip clubs and other forms of "adult" entertainment are immoral and should be outlawed. His views reflect the tenets of his faith and are shared by the members of his congregation. Now assume that someone, for some reason, decides to "cause trouble" for Minister Doe. This person visits a strip club in Ada, takes digital photographs of men in the audience and uses software to morph the image of one of the men into that of Minister Doe. This person posts the morphed photographs on a website, with captions announcing that Doe attends strip clubs; the person emails the link to the website to members of Doe's congregation and to other websites. The publication of these false images will inflict serious—perhaps irreparable—harm on Doe's reputation. While the images are in a sense analogous to the false textual allegations leveled at Wagner, they will almost certainly be more devastating because they are more compelling; advances in technology notwithstanding, most people still believe "seeing is believing," so they will tend to assume the photographs are true unless and until Minister Doe convinces them otherwise. This puts him in a very difficult position; unless and until he can prove a negative—prove it is *not* him in the photographs—an expanding audience will come to believe he is "the Baptist minister who likes strippers." The online dissemination of the photographs will almost certainly result in his being removed from his position, at least while the matter is being investigated; and it could result in his ordination being suspended or even revoked, if he is unable to discredit the photographs.

This may seem an extreme example, but it is not. It merely takes the online publication of defamatory material to the next logical level—to graphical, instead of or in addition to, textual defamation. It is—or will soon be—equally possible to use morphed video, posted on a site like YouTube,[319] to publish false video "allegations" about someone. The availability of graphical defamation further exacerbates the harm associated with online publication and further differentiates it from the MSM publication the drafters of the Model Penal Code assumed.[320]

The real significance of the Doe hypothetical, however, lies in what it reveals about the nature and consequences of the harm associated with reputational injury and with ridicule. In parsing the harms, it is useful to note that civil defamation law has not required proof of actual harm to establish a communication as defamatory.[321] Since this approach is consistent with criminal law's emphasis on controlling socially-undesirable behavior by sanctioning categories of behavior,[322] we will utilize it in this analysis.

When the Model Penal Code drafters analyzed the need to criminalize defamation, they assumed the only unaddressed harm was what we are calling ridicule and what they called gossip (less than reputational harm). They made this assumption because, as we saw earlier, they also assumed that filtered-MSM publication would (i) prevent the publication of most defamatory material and (ii) ensure civil redress for reputational harm inflicted when the filters failed. The architects of the Model Penal Code equated MSM publication with the infliction of reputational harm on the reasonable assumption that the oral, face-to-face circulation of even scandalous allegations is unlikely to inflict real reputational harm for the reasons noted earlier.[323] In their minds, then, the residual category of defamation—ridicule (or gossip)—was not an appropriate focus of criminal liability because the harm it inflicted was too minor to justify the imposition of penal sanctions.

---

[319] *See* YouTube, http://www.youtube.com/index (last visited Oct. 14, 2007).

[320] In addition to assuming the model of MSM-filtered publication examined earlier, the drafters would have implicitly equated "defamation" with the publication of textual material, given the then-very-limited sophistication of photographic and video technologies.

[321] *See* RESTATEMENT (SECOND) OF TORTS § 559 cmt. d (1977) ("[I]t is not necessary that the communication actually cause harm to . . . reputation. . . . Its character depends upon its general tendency to have such an effect."); *see also id.* at cmt. e (discussing the standard used to prove defamation). The extent of the injury is relevant in calculating damages.

[322] *See* Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, *supra* note 11, at 6-46.

As we have seen, these assumptions have been seriously eroded, if not completely invalidated, by the development of computer technology and the ever-expanding influence of the Internet. The result—at this point in our experience with computer technology—is that we need to revise their decision not to criminalize defamation in part, but not in its entirety.

Even though it has moved online and beyond the reach of filters, the residual category of defamatory harm we are calling ridicule is still not (and probably never will be) an appropriate focus of criminal liability. It is simply too mundane and too subjective to become the predicate for criminal sanctions.

As to its mundanity, consider Ghyslain Raza: The humiliation he endured was but an amplified version of what he would have experienced if some of his classmates had happened to observe him playing Jedi Master; their account of what they saw would have made Raza an object of amusement (ridicule) as it rippled through the school and, perhaps, somewhat beyond. The oral account would not have spread around the world, as the video did; we will assume, for the purposes of analysis, that the expanded scale on which the ridicule circulated aggravated the psychic harm Raza suffered.[324] But this is still simply a variation—a presumably enhanced variation—on the kind of experiences we have been dealing with as long as humans have lived in social groupings. Law cannot, as the drafters of the *Restatement on Torts* noted, eliminate the indignities and "petty oppressions" that are an inevitable, integral part of human society.[325]

---

[323] As we saw in Part III(C), when defamatory allegations circulate orally in a community, the members of the community can assess the merits of the allegations critically, in light of the experiential information they have about the person to whom the allegations pertain. False allegations are therefore likely to be less damaging than when they are circulated by more formal, and therefore ostensibly more credible, means.

[324] This assumption may be problematic. News stories about the "*Star Wars* Kid" emphasized the harm—the ridicule—Raza suffered at the hands of his classmates. *See, e.g.*, Ha, *supra* note 106. While Raza was obviously aware that his performance had been viewed by millions of people around the world, he did not personally interact with those people and so was probably ignorant of and/or able to ignore their reactions. If this is true, then the fact that online ridicule circulates more widely than face-to-face ridicule may be irrelevant in assessing the actual harm it inflicts.

The subjectivity of ridicule goes to the severity of the harm it inflicts. If Jane posts a video on "YouTube" that shows her roommate Mary drunk and vomiting, does this make Mary an object of ridicule or is it a shared joke?[326] The answer will depend on the subjective reaction of the ostensible victim; and how Mary reacts to the posting will be a function of many variables, including her personality and life experiences, her relationship with Jane, and other contextually idiosyncratic factors. As this example illustrates, criminalizing ridicule would require us to draw an inherently arbitrary line between joking and crime, between "blowing off steam" and crime, and between expressing an unflattering opinion and crime.[327] Criminal law has recognized that the infliction of psychic harm can justify the imposition of criminal liability,[328] and has therefore outlawed stalking and harassment.[329] It has not, however, predicated the imposition of such liability on the infliction of self-diagnosed psychic injury; stalking and harassment statutes incorporate a "reasonable person" standard, so the imposition of liability is based not on the idiosyncrasies of the victim but on conduct that can objectively be deemed to inflict harm.[330]

Courts have found that the inclusion of this objective standard prevents these psychic harm statutes from being void for vagueness.[331] The inclusion of such a standard is possible because stalking and harassment are "conduct" crimes, rather than "result" crimes.[332] Though both offenses derive from the need to deter the infliction of psychic harm, they do this by targeting continuing conduct that deviates from normal behavior and so can be described with a fair degree of objectivity.[333] We could not incorporate such an objective standard into a statute criminalizing ridicule because it would define a result crime, like assault; the goal would be to proscribe inflicting psychic harm—by a single act of publication—rather than a sequence of conduct inferentially likely to result in the infliction of such harm. Unlike assault, in which the proscribed result is *bodily* harm, the result proscribed by a ridicule crime would necessarily be capricious—the psychic harm a function of the varying sensibilities of specific individuals. Any attempt to criminalize the online (or offline) infliction of ridicule would undoubtedly be held unconstitutional: void for vagueness.

---

[325] RESTATEMENT (SECOND) OF TORTS § 46 cmt. d (1965).

[326] *See Roommate Puking*, YouTube, http://www.youtube.com/watch?v=GfrHDz_PrlM&search=sandbag (last visited Jan. 14. 2007).

[327] The drafters of the *Restatement of Torts* recognized this problem and sought to accommodate it with distinctions articulated in their commentary. RESTATEMENT (SECOND) OF TORTS § 559 cmt. b, 566 cmt. d (1977).

[328] *See supra* note 316 and accompanying text.

[329] *See, e.g.*, 11 DEL. CODE ANN. tit. 11, § 1311(a) (2001); IDAHO CODE ANN. § 18-7906 (2004); MICH. COMP. LAWS ANN. § 750.411h (West 2004).

[330] *See supra* note 329.

[331] *See, e.g.*, People v. Cross, 114 P.3d 1, 7 (Colo. Ct. App. 2004) *rev'd*, 127

The drafters of the Model Penal Code were, and still are, correct: There is indeed a *de minimis* category of defamatory speech, the criminalization of which would be bad law and bad policy. Ridicule is ultimately too common, too unstable definitionally, and too trivial to become the predicate of criminal liability.

This is not true of defamatory speech that inflicts reputational harm. More precisely, it is not true of defamatory speech the online dissemination of which inflicts more than *de minimis* reputational harm (since one can argue that ridicule inflicts a type of reputational harm). As explained earlier, the

---

P.3d 71 (Colo. 2006); State v. Partowkia, 96 Wash. App. 1027 (Wash. App. 1999); *see also* State v. Bryan, 910 P.2d 212, 220-21 (Kan. 1996).

[332] *See, e.g.*, Eugene R. Milhizer, *Justification and Excuse: What They Were, What They Are, and What They Ought To Be,* 78 ST. JOHN'S L. REV. 725, 805 (2004) ("When a criminal statute's purpose is to prevent a harmful result, the crime is said to be a result crime; when its intent is to prevent potentially harmful conduct, the crime is said to be a conduct crime.").

[333] *See, e.g.*, 11 DEL. CODE ANN. tit. 11, § 1311(a) (2001); IDAHO CODE ANN. § 18-7906 (2004); MICH. COMP. LAWS ANN. § 750.411h. Stalking and harassment are sometimes described as "course of conduct" or "continuing course of conduct" crimes. *See, e.g.*, Rodriguez-Cayro v. State, 828 So.2d 1060, (Fla. Dist. Ct. App. 2002); Burnham v. State, 761 A.2d 830, 831 (Del. 2000).

drafters of the Model Penal Code assumed, no doubt correctly, that civil liability sufficed to redress and discourage the infliction of reputational harm when publication was controlled by the MSM. As we also saw earlier, cyberspace invalidates the empirical premises on which that assumption was based; in cyberspace, publication becomes democratic and proletarian. It is neither accurate nor reasonable to assume that what is published will be filtered by professional staff or that one harmed by the publication of seriously defamatory material can obtain adequate civil redress from the publisher of the material.

The opportunities for the unfiltered publication of seriously defamatory material are therefore expanding while the disincentives for engaging in such publication are disappearing. To grasp the significance of these developments we need only consider the Doe hypothetical outlined above. The hypothesized harm Doe sustained is analogous to that produced by a physical assault. Here, it is not just Doe's ego that has been injured;[334] the publication of the defamatory photographs inflicted potentially devastating, perhaps ultimately irremediable harm on his "relational interests"—his reputation.[335] To remediate that harm, Doe will have to find some way to rebut the false allegations the altered photographs make. Even if he comes forward, publicly, with credible evidence showing that he does not attend, has never attended, strip clubs, some will not believe him; they will believe what they "saw," not what he says.

The Doe hypothetical illustrates one way, one of many, many ways, in which online publication can be used to inflict serious reputational harm. The drafters of the Model Penal Code recognized this harm, but chose not to criminalize its infliction for the reasons noted earlier, *i.e.*, the unlikelihood of its being inflicted and the availability of civil redress when it was. The increasing likelihood of its infliction and the increasing unavailability of civil redress require that we revise that decision and use a narrowly-focused form of criminal liability to deter online publication that inflicts serious reputational injury.[336]

---

[334] *Cf. supra* note 307 and accompanying text (explaining how defamation can cause injury to one's self-image).

[335] *See supra* notes 255-57 and accompanying text.

We must therefore do what the drafters of the Model Penal Code did not: craft an offense that encompasses the infliction of the proscribed harm without sweeping too broadly. As we all know, substantive offenses consist of three definitional elements: (i) *mens rea*; (ii) *actus reus*; and (iii) harm.[337]

The *mens rea* for our postulated offense should be equivalent to that required for the other psychic harm offenses, stalking and harassment. Both require that the perpetrator have acted with the highest level of *mens rea*, *i.e.*, intentionally, purposefully or maliciously.[338] These and other terms used to define aggravated *mens rea* are reducible to the requirement that a perpetrator have acted with the purpose of inflicting the proscribed harm on the victim.[339] The inclusion of such a stringent *mens rea* requirement is an essential prophylactic measure when we are dealing with the infliction of psychic harm. Lesser mental states may suffice when the harm is tangible, as with homicide; but when it is psychic a heightened *mens rea* requirement helps ensure that liability is imposed only upon those who acted malevolently.[340] Such a requirement also serves to limit the chilling effect an offense such as the one we are postulating can have upon speech; speech can provide the basis for the imposition of criminal liability, but to limit the chilling effect this can have, law requires that the speech be purposeful, *i.e.*, be consciously intended to result in the infliction of a proscribed harm.[341] Our postulated criminal defamation offense therefore requires that the perpetrator have published defamatory material online with the purpose of harming the victim's reputation.

---

[336] This is the approach that has been taken by at least some of the proposals to revise defamation law. *See, e.g.*, UNIF. CORR. OR CLARIFICATION DEFAMATION ACT § 1 (1993); ANNENBERG LIBEL REFORM ACT § 2(b), *reprinted in* SMOLLA, *supra* note 248 at § 9:96.

[337] *See, e.g.*, LEFAVE, *supra* note 201, § 1.2.

[338] *See, e.g.*, Nga B. Tran, Note, *A Comparative Look at Anti-Stalking Legislation in the United States and Japan,* 26 HASTINGS INT'L & COMP. L. REV. 445, 453-54 (2003).

[339] *Id. See also* MODEL PENAL CODE § 1.13(12) (1962) (defining intent as acting with purpose).

[340] The difference between the two lies in an issue the drafters of the Model Penal Code cited: the relative likelihood harm will be inflicted. The infliction of physical harm upon persons, property and/or animals requires a degree of physical effort and results in a clearly-identifiable degradation of a physical state; both inferentially support the propositions that the harm was actually inflicted and was inflicted inappropriately. As we have seen, with psychic harm it is possible that neither of these propositions will be true; the conduct involved in the infliction of such a harm may be quite trivial compared to that required for physical harm, and the resulting harm may, at least in some instances, be open to inter-

The *actus reus* for our postulated offense is the act of publishing defamatory material online.[342] That may seem straightforward, but it probably is not. One issue immediately becomes problematic: What does it mean to publish defamatory material online? Do I commit this offense if I post material that clearly inflicts serious reputational harm, with the purpose of inflicting such harm, in, say, a password-only accessible chatroom? Would that constitute publication? Or should publication consist only of disseminating material such as this in the truly public areas of cyberspace—areas such as publicly-accessible websites? Publication probably should be defined as encompassing both scenarios, if only because it is reasonable to assume that one bent on causing reputational harm to another would not post defamatory material in a limited-access area unless the poster had good reason to believe this mode of disseminating the material would achieve the desired result.[343]

---

pretation or dispute. It is therefore prudent to impose a higher *mens rea* for crimes targeting the infliction of psychic harm.

[341] *See, e.g.*, Brenner, *Complicit Publication*, *supra* note 29, at 324.

[342] We are assuming the offense is limited to online publication because the MSM still controls the real-world venues of publication. The assumptions the drafters of the Model Penal Code made therefore still hold for real-world, MSM publication, so criminal liability should not be needed in this context.

[343] This possibility illustrates yet another way in which MSM publication and online publication diverge: MSM media or mass media utilizes the blanket, indiscriminate publication of standard content; this mode of publication is a function of the one-to-many publication modalities (radio, television, print media) MSM utilizes. Online publication can be much more focused; it can, as in the scenario noted above, target particular interest groups, which can be even more devastating than the indiscriminate dissemination of content associated with MSM. With online publication, the distributor of defamatory material can target groups that

The third and most amorphous element is the harm. Crafting an offense such as the one we are postulating requires that we distinguish serious reputational harm from ridicule and do so with a level of objectivity sufficient to prevent the offense from being void for vagueness. How should we do this? We cannot rely upon the approach used in existing criminal defamation statutes because they either (i) conflate reputational harm with ridicule[344] or (ii) criminalize publications that "provoke a breach of the peace."[345] The second approach is based upon an empirical rationale that no longer applies.[346] And the first approach is analytically imprecise; it ignores the essential distinction we have drawn between mere ridicule and true reputational harm, presumably because these statutes merely incorporate the common law standard.[347] The reference to ridicule in the common law standard is clearly surplusage, since real concern under common law libel was with injury to the victim's reputation.[348]

The best way to define the harm in our new version of criminal libel, therefore, is to retain this emphasis upon injury to reputation and strip out all references to collateral issues, such as ridicule.[349] The offense therefore consists of purposely publishing material online that harms another's reputation.[350]

---

are likely to be particularly influenced by the material, which can enhance the magnitude of the harm inflicted.

[344] *See, e.g.*, COLO. REV. STAT. ANN. § 18-13-105 (West 2005); *see also supra* Part II.A.

[345] *See, e.g.*, ALA. CODE § 13A-11-160 (2005); *see also supra* Part II.A.

[346] *See supra* note 300 and accompanying text.

[347] *See, e.g.*, IDAHO CODE ANN. § 18-4801 (2004) (containing language that dates back to at least to 1864); *see also* Taylor v. State, 4 Ga. 14 (Ga. 1848); People v. Jerome, 1 Mich. 142 (Mich. 1848); State v. Neese, 4 N.C. (Taylor) 691 (N.C. 1818).

[348] *See, e.g.*, State v. Hoskins, 62 N.W. 270, 271 (Minn. 1895); State v. Boogher, 3 Mo.App. 442 (Mo. Ct. App. 1877); *see also* ANNENBERG LIBEL REFORM ACT, *supra* note 336, at § 2 cmt. ("common law evolved many colorful pejoratives to define 'defamatory,'" such as "hatred," "contempt" and "ridicule").

[349] In the analytical scheme we have developed, ridicule constitutes a lesser-included, albeit un-criminalized, level of defamatory harm; harm to one's ego, rather than harm to one's reputation.

[350] The proposed standard limits publication to online publication, because that is the focus of this article. It could, however, be expanded to include any type of

We then define reputation as one's "relational interest."[351]

Some might argue for differentiating between harm to one's personal reputation and to one's professional reputation, presumably on the premise that the latter is likely to result in the infliction of greater financial harm. This distinction may well be reasonable in the context of civil defamation law, which must calculate damages once harm has been proven. Criminal law, however, is concerned with harm as a generic, categorical concept, rather than as a fiscal construct; this focus on categorical harm derives from criminal law's central objective, which is the maintenance of social order.

There is another argument against attempting to differentiate personal and professional harms. It stems from the difficulty of parsing the two. Take the Doe (the minister alleged to have been in a strip club) hypothetical we began this section with, for example. The posting of the morphed photographs obviously, and intuitively, caused harm to Doe's reputation, but how would we parse that harm? Given the nature of Doe's profession, it is inferentially apparent that the publication of the photographs caused serious harm to his professional reputation, but would it not also damage his personal relationships? It is reasonable to assume that for Doe—as for most of us—there is no clear-cut, absolute point of demarcation between his personal and professional lives. Doe's personal relationships are likely to intertwine—associationally, emotively, and conceptually—with his professional ethos, status, and activities. It would therefore be difficult to parse the respective quanta of professional and personal harm that he sustained.

There is yet another reason not to differentiate, in any formal sense, between the personal and professional harm inflicted by a particular online publication; to do so might imply a hierarchy of harm, one in which professional harm is more important, more significant than personal harm. While

---

publication.

[351] *See supra* notes 256-57 and accompanying text; *see also* BLACK'S LAW DICTIONARY 1331 (8th ed. 2004) (defining "reputation" as "[t]he esteem in which a person is held by others").

such a hierarchy might make sense in the civil arena, where the calculation of damages is involved, it would be inappropriate in criminal law, where the emphasis is on deterring categorical harms. To understand why that is true, assume a variation of the Doe hypothetical. In this version of the hypothetical, the victim is Jane Doe, an Indiana housewife.[352] Jane has an undergraduate degree in education but has never worked in that field; she has chosen to work at home as a wife and mother. Jane and her husband lead a very conservative lifestyle; they are deeply religious, dress conservatively, drive a conservative car, and avoid sexually-explicit movies, music, television programs, and reading materials. Jane was, therefore, shocked and horrified when a friend sent Jane a link to a website which displayed morphed, nude photographs of Jane Doe engaging in a variety of sexually-explicit acts. Since she does not work outside the home, Jane presumably has no professional reputation which means she has merely sustained harm to her personal reputation. Can we, though, say that the harm she suffered was in some way inferior to that suffered by one whose professional reputation is the target of online defamatory material? Since the focus of the offense we are postulating is on the infliction of psychic harm, it seems that the precise nature of that harm should not matter as long as it impacted upon the victim's relational interest.

We should follow the lead of stalking and harassment statutes and limit our postulated defamation offense to cases involving the infliction of serious reputational harm. This further narrows the availability of criminal liability by eliminating instances in which reputational harm was inflicted but the harm was relatively trivial. Stalking and harassment statutes, which also seek to deter the infliction of psychic harm, achieve this goal by limiting the offense to conduct that inflicts "severe" or "substantial" emotional distress rather than mere emotional distress.[353] Our postulated defamation offense should therefore limit the imposition of criminal liability to cases in which the publication of the defamatory material inflicted serious or substantial reputational harm. As with the determination of whether emotional distress was severe or substantial in harassment or stalking cases, the determination of the severity of the reputational harm inflicted in a given case would ultimately be a matter for the jury to determine, using their native intelligence and everyday experience.[354]

---

[352] The Jane Doe hypothetical is based on an actual event with which the author is familiar, having been contacted by the woman who was victimized by the online publication of false photographs.

[353] *See, e.g.*, 11 DEL. CODE ANN. tit. 11, § 1311 (2001); FLA. STAT. ANN.

We need to note one other component of our postulated criminal defamation offense before turning our attention to its enforcement. The material alleged to be defamatory must be false;[355] as we saw earlier, the publication of true material may very well inflict psychic harm, but it is not a *defamatory* psychic harm. It seems to represent a new type of harm, since, as was also explained earlier, it usually does not constitute invasion of privacy, at least not as that harm has so far been defined.[356] The harm (if any) that people like Steinbuch suffer is not an invasion of privacy but a loss of control over information they prefer not to share with everyone.[357] We might want to craft an offense that addresses this emerging harm since it cannot logically be brought within the concept of criminal defamation.

The material must not only be false, the person responsible

---

§ 784.048 (2000); MONT. CODE ANN. § 45-5-220 (2004); WASH. REV. CODE ANN. § 10.14.020 (West 2002). The *Restatement of Torts* imposes a similar requirement in civil suits seeking damages for the infliction of emotional distress. RESTATEMENT OF TORTS (SECOND) § 46 cmt. j (1965).

Stalking and harassment statutes generally do not define substantial or severe emotional distress, but one court noted that it denotes "something more than everyday mental distress or upset." People v. Ewing, 90 Cal. Rptr. 2d 177, 184 (Cal. Ct. App. 1999).

[354] *See, e.g.*, Snowden v. State, 677 A.2d 33, 38 (Del. 1996).

[355] *See supra* Part IV.A.1.b.

[356] *See supra* Part IV.A.1.b.

[357] *See, e.g.*, ADAM GREENFIELD, EVERYWARE: THE DAWNING AGE OF UBIQUITOUS COMPUTING 126-28 (2006). Greenfield notes that "we've historically built our notions of reputation such that they rely on *exformation*—on certain kinds of information leaving the world, disappearing from accessibility." *Id.* at 128. It is this interest, this concept that sustains harm in scenarios such as the Steinbuch-Cutler saga.

for publishing it online must also have known it was false when he or she published it. This is consistent with our requiring that the perpetrator have acted with the *purpose* of inflicting reputational harm on the victim. The falsity of the material is an attendant circumstance essential to the commission of this offense; under the Model Penal Code, therefore, the perpetrator must have known that the material was false, believed it was false, or hoped it was false.[358]

B. Enforcement

We have decided that a narrowly-focused defamation offense should be incorporated into the criminal law, in part because civil liability is not an effective means of controlling online defamation. Some may point out that efforts to impose criminal liability will encounter at least some of the same obstacles that impair civil liability's efficacy in this context. The fact that a perpetrator is judgment-proof is not relevant when criminal liability is involved, but his or her ability to remain anonymous is. Another issue that can complicate enforcement—one that also arises in civil defamation suits—is the problem of jurisdiction, which becomes particularly difficult when online publication is involved.[359]

The legal analyses required to resolve these issues are both complex and quite outside the scope of this article. This section has a much more limited objective: to speculate about how a very old notion could be revived, modified, and used as an enforcement device when anonymity, and/or jurisdiction bar the use of more conventional measures.

Our speculation begins with the proposition that the defamation offense we postulated above differs somewhat from other offenses involving the infliction of harm. The infliction of harm has historically been the prerogative of a human being. The human can use implements (gun, knife) to inflict the harm, but there has been a necessary correlation between human actor and the resulting infliction of harm. Guns do not shoot themselves and knives do not stab unaided. Humans can use certain implements to inflict harm remotely but there still tends to be a rough one-to-one correlation between human effort and resulting harm.

---

[358] *See* MODEL PENAL CODE § 2.02(2)(a) (1962). This requirement ensures that the statute is constitutional under the *Garrison* holding. *See supra* Part II.C. This may not be important because the postulated offense is intended to be used primarily when private citizens are victimized. As was noted earlier, the *Garrison* holding does not apply to when the victim is a private citizen. *See supra* note 80.

[359] *See, e.g.*, Eric Barendt, *Jurisdiction in Internet Libel Cases,* 110 PENN ST. L. REV. 727 (2006).

Online defamation is different. The human perpetrator of an act of online defamation publishes the defamatory material by posting it, somehow, online. Once posted, the material remains online unless and until it is removed, either by the perpetrator or by someone else. One of the issues that would arise in enforcing our postulated defamation offense would be the removal of the offending material; as long as it remains accessible online, the harm is still being inflicted and the crime is still being committed.

This does not mean that, if we decide to implement the defamation offense, we should not focus on apprehending, trying, convicting, and sanctioning the perpetrator. Here, as in other areas of criminal law, our ultimate goal is to exercise enough control over human behavior to maintain a baseline of social order; we do this by creating disincentives for individuals to engage in proscribed behaviors.[360] And we create these disincentives by sanctioning at least a subset of the individuals who engage in these behaviors; we deprive them of their ability to re-offend by incarcerating them; and, in so doing, hope to discourage others from engaging in similar activity.

This approach has worked satisfactorily for other offenses and should work satisfactorily for our hypothesized defamation offense, as well (assuming we can identify and apprehend the necessary sub-set of perpetrators). The residual, perhaps unique problem is that even if all this functions perfectly, the offending material may still be online, harming the victim. (This will, no doubt, also be true if none of the enforcement methods function as they should because of jurisdictional obstacles, the perpetrator's persistent anonymity or other issues.)

---

[360] *See* Brenner, *Toward A Criminal Law for Cyberspace: Distributed Security*, *supra* note 11, at 6-46.

One way to deal with this residual problem would be to require the perpetrator to remove the offending material. The statute defining the offense could impose such an obligation on convicted perpetrators, if necessary, and could provide for the imposition of special or enhanced sanctions when a perpetrator refused to comply. This assumes that the perpetrator (i) has been apprehended and (ii) is able to remove the offending material. Neither may be true: The authorities may be unable to apprehend the perpetrator because he or she remains cloaked in an impenetrable anonymity or because jurisdictional or other procedural obstacles (such as the lack of an extradition treaty) prevent the authorities from obtaining custody of an identified perpetrator. Even if the authorities obtain custody of a perpetrator, he or she may not be able to remove the offending material or may be able to feign an inability to do so with credibility sufficient to convince the authorities. In the first scenario, the perpetrator has intentionally or otherwise lost control over the site in question; in the second scenario, the perpetrator has structured the procedures by which he or she gains access in such a way that it seems he or she has lost control over the site in question.

All of this assumes that the perpetrator has been apprehended. Given the capacity one has to remain anonymous or pseudonymous online, it is likely that some (many) perpetrators will not be identified and apprehended.

Both scenarios present the very real possibility that the apprehension of the perpetrator cannot result in the removal of the offending material, which means that the commission of the crime—the infliction of harm upon the victim—continues unabated. This, unfortunately, is a possibility we may have to confront in other areas as well, as the ever-accelerating evolution of technology produces software, and hardware, that is capable of acting autonomously. Here, we are confronted with a very passive example of this automated, remote infliction of harm. While it is a primitive instance of automated harm, the continuing infliction of reputational harm by online defamatory material requires us to consider how we will approach object-as-perpetrator or process-as-perpetrator, and, perhaps, gives us an opportunity to experiment with solutions we can implement if and when automated harms become more common and more sophisticated.

Assume, therefore, that the perpetrator in the Minister Doe hypothetical (a) cannot be identified and apprehended or (b) has been identified, apprehended and convicted but claims he cannot remove the offending photographs. Assume also that the site on which the offending photographs are posted disclaims any responsibility for removing them. Does this end the matter? Is this an acceptable resolution?

Arguably, at least, it is not. Even if the perpetrator has been apprehended, convicted, and is being sanctioned for posting the photographs, his crime is still being committed. Our model of law enforcement assumes that the commission of a crime does not survive the arrest, prosecution, and conviction of the perpetrator, either because (i) the commission of the crime was concluded long before those processes began or (ii) the apprehension of the perpetrator terminated the commission of the crime. The termination of crimes is an essential, assumed component of the model's efficacy in controlling crime; aside from anything else, the termination of crimes establishes law enforcement's ability to maintain social order.[361] If the perpetrator's conviction and sanctioning do not result in the termination of his crime, we have a disconnect which suggests that the process is somehow incomplete (and therefore unsatisfactory).

How can we resolve this residual problem—the persistence of reputational harm to the victim of online defamation? One possible solution is to approach the object-as-perpetrator or process-as-perpetrator as a target—an incremental target in this context—of criminal liability in its own right. If the offending material (object-as-perpetrator) is approached in this fashion, it creates the possibility of law enforcement's taking direct action against that material, instead of its having to act indirectly, via the perpetrator (which, of course, may prove satisfactory in many or even most cases).

---

[361] *See id.*

Conceptually, how could we establish the object-as-perpetrator? Except for corporate and other artificial, human-composite entities, our criminal law is concerned with individuals, not objects (or processes). We do have doctrines in place that allow for the forfeiture of objects that played a role in the commission of a crime.[362] Some of these doctrines are based on the fiction that the object in question was itself guilty of a crime.[363] Forfeiture, however, is based on the premise that the property is to be seized because it is tainted by its association with the commission of a crime and it has some value.[364] We are dealing with a very different issue—with the fact that the object (or process) itself is (still) committing the crime; our goal, therefore, is not to seize the property because of its value, but to interrupt its continuing the commission of the crime.

How can we justify taking direct action against the object (or process) that continues the commission of the crime? There are ancient doctrines, such as the deodand, under which animals and objects were regarded as capable of committing crimes in the same way and to the same extent as human beings.[365] These ancient doctrines, which seem very strange to us, imposed the same standards of criminal liability and the same criminal adjudicative procedures on animals and objects as upon human actors.[366] These extinct doctrines were the product of cultural forces that are quite foreign to us and are therefore quite inapposite, in a literal sense, to the issues that confront us. However, they may suggest an instrumental approach we could utilize to deal with the scenario currently before us (online defamatory material's continuing to inflict harm on the victim) and other emerging instances in which technology gives rise to automated crime.

---

[362] *See, e.g.*, United States v. Bajakajian, 524 U.S. 321, 329-32 (1998).

[363] *See id.*

[364] *See id.*

[365] *See, e.g.*, Paul Schiff Berman, Note, *Rats, Pigs, and Statues on Trial: The Creation of Cultural Narratives in the Prosecution of Animals and Inanimate Objects*, 69 N.Y.U. L. REV. 288 (1994).

[366] *See id.*

We *could* develop a doctrine that allows for the imposition of a type of criminal liability[367] upon online defamatory material that would justify law enforcement's taking direct action to remove or otherwise terminate the material's capacity for inflicting harm upon a victim. The imposition of the liability could supplement the liability imposed upon the human perpetrator who actually published the material online when the perpetrator has been identified and convicted, or it could serve as a substitute when the perpetrator cannot be identified or apprehended. As to the type of direct action it authorizes, this object/process liability could justify law enforcement actions when official demand that the operator of the website where the material is posted, the entity hosting the site, or some other responsible party see that the material is removed or face the prospect of being convicted as an accomplice to a crime in process. It might also—and this could be very controversial—justify law enforcement's taking direct action to remove the material or alter it so that it could no longer communicate defamatory content.

V. CONCLUSION

The increasing incidence, virulence and creativity of problematic online speech—including defamatory online speech—are visible manifestations of how cyberspace and computer technology are changing our societies. Cyberspace and the technologies that support it are responsible for an emerging, fundamental shift in power. Power, such as the power to control publication, was historically concentrated in hierarchical commercial and governmental entities. As we have seen, cyberspace changes that; it erodes, and will no doubt ultimately disassemble, the MSM's domination of publication.

This creates new opportunities for the infliction of psychic harms, a phenomenon with which the criminal law has had little experience and of which, until relatively recently, it took little cognizance, for reasons the drafters of the Model Penal Code noted. The infliction of psychic harms used to be limited to face-to-face encounters, which inevitably import identifiability and an attendant level of accountability; the result was that the harm inflicted was generally muted. The anonymity that we can enjoy online frees those who are so inclined to inflict greater levels of psychic harm on those they select as victims. This creates difficult challenges for criminal law, as we have seen in this article. On the one hand, criminal law cannot address every slight, every insult, every hurt feeling; on the other hand, psychic, intangible harms can be as devastating, if not more so, as more traditional, tangible harms.

---

[367] It would have to be strict liability since we, anyway, would not impute *mens rea* to objects or processes. Alternatively, the *mens rea*, and the *actus reus*, too, for that matter, might be derivative: based on the conduct and (inferred) intent of the person responsible for posting the material.

Criminal law needs to develop a taxonomy of psychic harms. This article deals with one such harm: defamation. In so doing, it distinguishes the harm inflicted by defamation from privacy-related harms. What, though, is the precise relationship between defamation, privacy-based harms, stalking, harassment and other instances of psychic injury? How can we determine when a particular instance presents, say, an invasion of privacy versus an act of defamation? And is our current arsenal of offenses adequate to deal with the already-emerging varieties of psychic harms?

This article argues for incorporating a narrowly-focused, precisely-defined defamation offense into our criminal law. Should we also introduce a new privacy-based offense, one that deals with the dissemination of true information about someone? As explained earlier, the publication of this type of information does not (and should not) constitute invasion of privacy, but that does not necessarily mean it does not represent an invasion, a violation, of an interest we need to protect.

As the evolution of computer technology and its integration into our lives accelerates, it will become even more important to protect individuals from "information crimes." What is an "information crime?" Essentially, it is using information (or misinformation) to harm another person. Why should we be concerned about information crimes?

For most of our existence, we have interacted face-to-face. Face-to-face interaction lets us acquire the information we use to assess and interact with another person directly; we rely on our own observations and our own assessment of what we observe. We also, as explained earlier, rely on first-hand information that we obtain from others whom we know and trust. All of this is an active process; we gather, assess, retain, discard, and act on information about others. We have become very adept at using verbal and non-verbal data for this purpose.

We still adhere to this process and probably always will; however, this process is already being influenced by modern communication technologies. Employers, for example, "Google" prospective hires, and information that they acquire can affect the decision they make.[368] As informational technology becomes ever more pervasive, we will rely more and more on this kind of "canned" information in our interactions with others.[369] Before I meet with someone (or as I meet them) I will use a handheld device (or an implant) to do a quick check on them. Like the companies that currently rely on Google, I will assume the information I access is accurate, and so will rely upon it in my dealings with that person . . . just as some women already seem to be relying on entries posted on "Don't Date Him Girl" to screen potential suitors.

In a world such as this, the accuracy of the ambient information available to a person takes on great significance. It is therefore appropriate, and may become absolutely necessary, to use some level of criminal liability to ensure that this information is free from maliciously introduced falsehoods and distortions. The online defamation offense postulated in this article is offered as a first, conceptual step in this direction.

---

[368] *See, e.g.*, Erin White, *Recruiters Use Google to Screen Job Applicants,* COLLEGE JOURNAL, Oct. 18, 2004, http://www.collegejournal.com/columnists/thejungle/20041018-jungle.html.

[369] *See, e.g.*, GREENFIELD, *supra* note 357, at 86.

PANEL DISCUSSION I

THE DECISION TO PROSECUTE

INTRODUCTION

On April 5, 2006, as part of the Prosecutorial Responses to Internet Victimization Conference hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General, two panels were held to focus on pressing issues faced by prosecutors involved in Internet Victimization cases.

These articles are distillations of the two panels. The articles highlight especially relevant portions of each panel discussion and incorporate the speakers' actual words. For a number of practical reasons related to transforming a panel into an article, the panelists' remarks have been edited and, in some cases, changed or re-ordered for continuity and clarity. To convey the feel of the live panel, substantial block-quotes have been included which add to the realistic and practical tone of the panels. The panelists appeared on their own behalf to share their experience and insight. As such, their comments were solely their own and not on behalf of any agency or organization.

Both panels were moderated by the editor and consisted of experts who answered questions prepared prior to the conference before a spirited and insightful audience.

Marc M. Harrold[1]

PANELISTS:[2]

- Terry Berg, First Assistant United States Attorney, Eastern District of Michigan; former Chief, High Tech Crime Unit, Department of the Attorney General of Michigan
- Patrick Corbett, Professor of Law, Thomas M. Cooley Law School; former Deputy Chief, High Tech Crimes Unit, Department of the Attorney General of Michigan
- Todd Lawson, Assistant Attorney General, Office of the Attorney General of Arizona
- Thomas Sadaka, Of Counsel, Berger Singerman; former Assistant Statewide Prosecutor, Office of the Attorney General of Florida

"There's no way that any office can prosecute every case."

This statement was the starting point for a panel discussing the factors that contribute to a prosecutor's decision whether or not to prosecute a particular case involving Internet victimization. The Panel's goal was to provide information in an attempt to answer, or at least come to better terms with, the following questions:

QUESTIONS FOR PANEL:

1. What is the role of resources in the decision whether to prosecute?
2. What is the role of multiple jurisdictions (victims, perpe-

---

[1] Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.

[2] It should be made clear, at the outset, that the statements and opinions offered by the panelists and moderator are solely their own and are not offered on behalf of any organization or agency.

trators, witnesses, etc. and the varying levels of prosecuting agencies (i.e., federal, state, local)) to the decision whether to prosecute?

3. What role do the characteristics of Internet victims or their experiences play in the decision whether to prosecute?
4. What are the policies and procedures related to case acceptance or denial?
5. What are the challenges in dealing with law enforcement in Internet victimization cases?

QUESTION 1:

What is the role of resources in the decision whether to prosecute?

An underlying theme of the panel was that there are several major, limited resources that influence the decision to prosecute. The following discussion focused primarily on money, time, staff and technology.

PROFESSOR CORBETT stated from the outset that "budget is a massive concern in this area, whether it is setting up the [cyber-crime] unit, buying the equipment, and then having witnesses and victims that are all over the country." Internet victimization cases generally take a great deal of time. In some cases, administrators (i.e., "bosses") do not have the same level of interest, experience, or understanding of computer cases [as their subordinate prosecutors]. This can lead to under-prioritization or supervisor criticism that a prosecutor is spending too much time without yielding results. PATRICK CORBETT conveyed his experiences in Michigan:

> What I have seen in Michigan—and possibly this is occurring in your states—is unless you have prioritized this as an area for prosecution and have higher ups/bosses who understand the time it takes to be able to investigate and prosecute these cases and that you might do a lot of investigation for a lengthy peri-

> od of time, expend a lot of resources, and might not get anybody at all. You might find out that they're in Russia and you can't get them. Unless you have that mentality from the top down, it's difficult to do any cases other than sexual predator [cases].

It also came to light that it is not only the resource limitations of the attorney general's office, but also the resource limitations of the investigative agencies which may, or may not, be part of an attorney general's office that can influence the decision to prosecute. For example, in Florida, all of the investigators in that constituent office are civil investigators, leaving prosecutors somewhat at the mercy of decisions made by the administration of outside law enforcement agencies. In some cases, TOM SADAKA reported, the result was that no investigation took place at all: "Generally, [outside law enforcement agencies'] budget concerns are more of an issue because you can't even get them to invest the resources necessary to investigate the [computer crime] cases, because they're just too costly."

To illustrate this separation between prosecutors and law enforcement in the Internet victimization area, TOM SADAKA stated:

> A couple years ago I modified our identity theft statute to include a paragraph that said that the case could be investigated or prosecuted where the victim resided or where any element of the crime occurred. [This was] simply to make it easier for local law enforcement when their citizen victim called in and said, "Hey, I've been the victim of identity theft that happened in Utah."
>
> The local office no longer had to say, "Well, that's outside of our jurisdiction." The response I got, and this speaks directly to the budget, was hate mail from the sheriffs, and phone calls saying, "All right, so you're going to give us the money to go investigate these cases, too, now that you've made us do it?" I

> said, "Well, I really haven't made you do it. I've just created an avenue so that you can." But that's all purely a budgetary issue.

The following is a paraphrase of the ensuing conversation among the Panelists and audience:

> If you have fifty complaints, but twenty of them are on one guy, they'll package up those twenty consumer complaints for eBay fraud or for identity theft or however they're coming in. They'll package up twenty people and they'll send over to me and say, "Hey maybe this is a guy you can investigate." [This] helps keep us focused on the most-efficient cases. This is especially true from the detective's perspective.
>
> If you are a street detective and you're working an Internet crime beat or an identify theft beat, you almost have to work every little angle, because all the cases in this area start with one complaint on a small amount, $50.00 loss or a $500.00 loss. It's when you kind of get to the source of it and you look at the bad guy's computer and, whoa, he's ripped off 2,000 people at $50.00 a head or $500.00 a head—that's when you've bumped into the big case. It all happened because of one little victim. So you have to do a certain level of low-level service to victims to find the big cases that are going to be worth your budget draw.

The panel generally agreed that the decision to prosecute might come down to a type of pragmatic, objective determination. In many cases, that decision to prosecute will hinge on the ratio of a particular defendant's damage and the aggregate nature of the victimization, whether or not it is monetary. In making that decision to prosecute, distinct from the number of victims and where they are, a number of state statutes have thresholds. For example, if you want to charge an aggravated identity theft, you need to have five victims. So we'll start to look for cases that have that accumulation so that you can get up to more-serious charges. If we have one really loud victim who lost $50.00 versus eight or ten victims who each lost $50.00, you start to look for the collectives and the groups and the ways you can get more bang for your buck with the prosecution. Limited technological resources are also relevant and affect the type and number of cases that prosecutors' accept. Most prosecutors' offices are limited to the forensic area:

> I can find a detective somewhere to go knock on the bad guy's door. What I can't do is get anybody to search his computers between now and 2009. They're going to sit in a warehouse somewhere until the forensic guy gets around to it. So when we start looking at the victim complaints that come in, we try to do some aggregation.[3]

In certain instances, the legislature, eager to appeal to the timely concerns of its constituents, passes criminal statutes that will not realistically be enforced. When this occurs, it stretches existing limited resources even farther.

For example, PROFESSOR CORBETT made the following observation about Michigan laws:

> Something that has happened in Michigan, and I'm guessing this [has] happened in your states, is [that] the legislature sees a need to pass these new laws. Maybe it's because they just want to have something that says "children" in it and protecting children helps [them] to get re-elected. Especially in Michigan, [as] their terms are limited and maybe this is happening in your states [as well]. So they feel like they have to do something quick[ly], but you [end up with] all these laws.
>
> The clearest example of the budget being a con-

---

[3] This is a paraphrased version of conversation among Panelists and Moderator.

> cern is with statutes for crimes that no law enforcement officer is even remotely going to consider pursuing.
>
> Michigan recently passed the Children's Protection Registry Act.[4] I routinely go talk to law enforcement officers about state laws and update them on the laws, and they're like, "What? This is a criminal statute that exists? I don't know anything about it. I've never even heard of it." Then I ask "would you ever be able to prosecute a case under it?" [They respond], "Are you kidding me? I have no time for anything but the certain kind of cases that [my] boss[es] have made a priority." So that's the clearest indication that budget's a massive concern to me.

TODD LAWSON provided a final example of how limited resources, especially in victim/witness travel-in cases with a sizeable number of victims spread out geographically.

> We had an auction fraud case with 228 victims of baseball card and memorabilia related fraud. When it came time to charging I used a group count—a scheme count and I indexed all 228 as victims. Then, we sent them all notices.
>
> When it came time for trial, we whittled that list down to reflect a simpler pattern so we could make sure we still had enough incidents to prove a scheme. We had enough victims to show a pattern, and to make sure we had a loss threshold. Even if all 228 are not named in the indictment, it is important that they are all counted for purposes of a plea.
>
> If it comes to trial, I ask some of the people up front: "Are you willing to travel?" Usually, I get back the standard, "No, I'm not willing to travel." In that case I say, "Well I can't guarantee that you'll get restitution if we go to trial." This way the ball is back in

---

[4] *See generally* MICH. COMP. LAWS § 752.1061 (2004).

their court.

If we do get a plea, I can put them on the restitution. Of course, the defendant owes no telling how many people so it might be $50.00 a month for the next seven years while they're on probation. So, that may be a loser anyway.

I do believe that in a case where I have the defendant here, [in my jurisdiction] and I have a multitude of out-of-state victims, I'll put them on a count and try to get them victim rights. But, when it comes to trial, I will easily whittle it down to what I need to make a trial manageable. I won't call all 228 [victims].

We had a defendant who was doing large-scale identity theft, and all his victims had been customers of a medical center in northeast Louisiana. He'd obviously stolen some records, or had gotten some stolen records from [the medical center]. First, we had him in Phoenix. So, we prosecuted him there. All our victims were from Louisiana. I could also see the flipside. What if I was in Louisiana and I had a defendant somewhere else and I could make the case in Louisiana where he had stolen all the information? In that case I could bring that case where the victims are if I had a pattern like that.

I don't necessarily think that I need to have the defendant in my jurisdiction. Wherever the defendant is, his computer is. Wherever his computer is, there's a lot of evidence. It's hard for me to call up another state's law enforcement agency and say, "Will you do this for me?" The [U.S.] Postal [Service] guys pick up the phone and they're talking to guys they went through training class with. Being in the task force with the Postal guys makes all the difference. They task people.

I've forgotten how many times I've got a case that's heavily involved in the Fort Lauderdale area. We've found a number of the Postal guys out there basically doing work for the attorney general's office in

> Arizona, as a favor to the Postal Inspector in Phoenix. They've done countless hours of work for us. So, that's another advantage to task forces.

QUESTION 2:

What is the role of multiple jurisdictions (victims, perpetrators, witnesses, etc.) and the varying levels of prosecuting agencies (federal, state, local) to the decision whether to prosecute?

TODD LAWSON provided an initial synopsis:

> Every case starts off with one loud complainer who's got a $50.00 loss or a $500.00 loss, usually. You have to do a certain amount of due diligence in the beginning to see if it's going to break out into an organization, or if it's going to break out into a guy passing bad checks on the corner. If they have multiple outlets for a task force, the task force will be more efficient.
>
> Because if it's that one guy who is the homeless guy living on the corner who is passing bad checks, police will refer that to a county agency for a bad check. Taking that as an ID-theft investigation might lead to some of the types of cases we've had. We've found prison gangs running ID-theft operations and employees of county government running ID-theft operations.
>
> The more expansive kinds of cases gravitate towards the U.S. Attorney's offices side. So we kind of have the county attorney taking the little stuff and the U.S. Attorney taking the big stuff, and then we [the attorney general's office] get everything else. It works out fairly well in terms of good cases with moderate-sized losses, and usually anything that has an interstate or multi-state angle goes to the U.S. Attorney, so it makes things easier to prosecute. We have the big statewide crime, which is what we're aiming for.

The panel line-up was particularly valuable because there was an opportunity for state assistant attorneys general to discuss the role of the federal government in accepting or denying certain cases.

> In response to a specific question about the role of U.S. Attorney's Offices, TERRY BERG stated:
>
> > Well, here's the deal. As I'm sure all you know, I've been in the state system too. So, I've been on the outside looking in. The feds just don't handle as many cases as the states do. Let's face it—the states and counties do a ton more cases than the feds.
> >
> > So, the bulk of criminal prosecution in our nation is done by the locals and the states. There's no question about that. The other thing is that, and again, when I was thinking about this question of the role of the victim and the decision whether to prosecute, well the decision to prosecute is a broad concept.
> >
> > It means whether you even want to do the case or not, should we do the case or shouldn't we? It also, I think, encompasses the question of, "Well, what do [I] charge?" You think you're going to do the case, but now the questions emerge related to the decision to charge and, specifically, what charges to use?
> >
> > I see the role of the victim probably being more important in the latter area of the charging decision. How to actually craft the charges once you think you're going to bring the case. Because whether or not to prosecute is really, to me, based more on the strength of the evidence in the case, and then whether you have prosecution thresholds of some kind that determine whether or not you're allowed to take the case.
> >
> > This is sort-of my long way of getting into the federal system. We do have prosecution thresholds, which are usually in financial terms. In the fraud area, they relate to how much money was lost. Our prosecution thresholds are under review right now. By

way of example, let's say that the prosecution threshold for a fraud case was $100,000.00 or $250,000.00. Well then that means that the average identity theft case where someone's credit card was used or their identity stolen and a credit account was opened or some other kind of Internet account was opened, [and] financial damages were incurred, is not going to meet the threshold for a federal case.

So the bottom line is that if we wanted to try and look at it and say, "What kinds of cases would the U.S. Attorney's Office be more interested in or able to take?" The general rule of thumb is really big cases. They would be cases involving a lot of money, cases involving interstate commerce—all Internet cases are this way—but some serious interstate activity occurring in more than one state.

In some instances, these are going to tend to be the cases that most prosecutorial entities would rather keep themselves. Why, because they're really good cases. Due to limited resources, what the federal system tries to do is to narrow down its focus and take those cases that are the most significant.

That's one side of things. The other side though is that through the use of task forces, there can be a very effective sort of multiplier effect in terms of the investigations that can be done. That is a way to leverage federal resources.

Because many federal agencies will want to send a person to work on a state and local task force in the area of Internet crimes against children, those task forces often involve federal agencies. In our district, we have a very effective identity fraud task force that includes state and local officers.

The task force also involves the corporate security representatives of some of the big retailers, like Target®, for example. They've just been great. The task force agents have done a lot of great cases. They're very reactive. They work with certain prosecutors

> within the U.S. Attorney's Office, so they get warrants and do complaints right away. They almost work like a drug squad. They'll go out. They'll get information regarding a particular house where ID's are being made or checks are being made, and they'll hit the house. They'll develop information.
>
> They try to go after organizations basically, identity fraud organizations, which are also another sort of buzzword in terms of getting the feds involved. If you have a case involving an organization, a conspiracy, a group, then that's the kind of case that the feds are going to be wanting to focus on more than the individual cases.
>
> So that, I guess, is the bright side of things. Getting the U.S. Attorney's Office to take any particular case may be difficult unless the loss amount meets their thresholds, or the type of case that it is, is significant enough. Through [the use of] task forces, you can leverage pretty effectively.

One of the primary challenges in prosecuting Internet-related crime is that exposure in numerous jurisdictions is the norm, not the exception. Prosecutors who have usually only prosecuted cases of crimes committed in the jurisdiction they serve are now faced with victims, perpetrators, or witnesses who may reside in another state, or even another country. It may be fairly easy to decide to prosecute a perpetrator who stole $50 from 100 people in the same jurisdiction. Given the amount of $5,000, it would likely be a felony. But, how do prosecutors deal with a perpetrator who stole $50 from 100 victims but only one of those victims is in their jurisdiction? Which of the individual prosecutors' offices, given their limited resources, is going to pursue the misdemeanor committed in their jurisdiction?

The panel touched on the pragmatic concerns of the elected state attorneys general, for whom they (and the members of the audience) worked. Specifically, what is the interest, other than the general pursuit of justice, for an attorney general's office to pursue a defendant where no victim resides in that jurisdiction? TERRY BERG commented:

> The problem becomes: what is the interest, if you will, or how strong is the interest of the prosecutorial entity when there's no victim, when there's no harm occurring in the jurisdiction of that entity? Now that's a harder question, I think, for county prosecutors than it is for an attorney general's office, because then you have the whole state.

While the incentive to prosecute may be greatest in the jurisdiction where the victim lives, from a practical, judicial economy line of reasoning, TERRY BERG believed that it may be most effective to prosecute the case where the defendant resides:

> Generally speaking, the proper forum for the prosecution is the location where the defendant is, not necessarily where the victim is located. That's where the police are who can effectuate the arrest. Where the defendant is, that's where much of the evidence will be located.
>
> Where the defendant is, that's where the physical crime occurred, whether it is typing on the computer or sexually abusing someone. So, the proper venue is usually where the defendant is located.

A criminal investigation and prosecution for criminal activity that takes place in numerous jurisdictions is always challenging. TERRY BERG shared an in-depth example of a case involving a great number of victims and how this can be handled when the crime is very "widely spread" out:

> We had a case recently that was the enforcement of what's called the CAN-SPAM Act.[5] It's the federal

---

[5] *See generally* 15 U.S.C. § 7701 (2003); 18 U.S.C. § 1037 (2003).

Anti-Spam statute. Do any of you have state anti-spam statutes? I know a lot of states do now, with criminal, as well as civil, provisions.

Well, if you've done any of these cases, you know that they're very difficult in terms of how widely spread [out] they are. That's one of the key characteristics about them. Let me take a minute here and tell a little bit about [one] case. The defendant's name was Daniel Lin. It began with the Federal Trade Commission, which does a great job with their investigations. They had received a [number] of complaints regarding spam advertising medical products, various different medical products you see advertised on the Internet, including these diet patches and Viagra—they were selling Viagra that was manufactured in India. They were selling pills that were to enlarge certain portions of your anatomy. They were selling things like that. At any rate, there were all sorts of complaints. The question becomes, "How do we find out who is doing this."

As you can imagine, the method [the investigators] tried to use was [to] follow the money. They made some orders. Then they tracked where the money was being paid. They were able to determine that it was essentially being deposited into the account of an individual who was in Michigan.

In a CAN-SPAM violation case the issue is, as you know, "Okay, who's actually sending the spam?" not necessarily "who's benefiting financially from the purchases that occur when somebody who clicks on the spam goes to the website and makes a purchase."

So, you have a commercial connection but not necessarily the answer to the question of who is sending it. So, as the case developed, what we found out was that these folks were using "open-proxy computers."

Essentially, a proxy computer is just a computer that's on the Internet that other computers connect to for the purpose of going to the Internet. A lot of corporations and the government will have a proxy computer that when you go to the Internet you actually go to the proxy computer, and it is that computer that actually takes you to the Internet.

Well, if these proxy computers are left open, then they become like relay stations that the spammers use. They look for those open proxies. There is a whole black market for lists of open proxies. That's what these folks were doing in this case.

Fortunately, through the help of some of the victim's groups, [we] were able to make some headway. I think victim's groups can really be helpful in this area. There's one called "SPAM HAUS" that was able to essentially connect the investigators to a company that was in Germany that was running what they called a "proxy pot."

A proxy pot is a computer that's sitting on the Internet looking like an open proxy so that when [individuals] who are either selling the proxy lists, or otherwise just looking for open proxies by doing scans, they will find them. They find that set of IP numbers that appears to be an open proxy.

Then when the spammers go to do their blasts of spam and they send it to all these different open proxies, they actually sent it to this proxy pot that was located in Germany. So, once we were able to get the information from the company in Germany, we had the advantage of having the connection where the spam was actually originating from.

The reason they use the open proxies in the first place is that it hides the origin of the computer transmission. It looks as if it's coming from the open proxy computer, rather than from the person who's actually sending it.

So, with the help of the German company (the proxy pot company) we were able to determine who the actual "button-pusher" was. Who was the person actually sending the spam in this case?

This was because the company was logging all this information. That was the whole point of the proxy pot. That enabled us to say, "Okay, this is the person who is doing it?" This brings to light a number of different points about victims in this type of case.

If you think about a spam case, it is almost the epitome of a computer crime case. It brings into play all of these different questions and problems as it relates to victims. The one point is [that] if you look at what cracked the case, it was the German company with the proxy pot that enabled us to say, "Okay, now we can track back to Daniel Lin and his cohorts who were sending the spam."

So, the company is actually a victim. That's a cooperative victim, because that proxy pot was sitting out there on the Internet, just like all of those other open proxies, but it's just that they were intending to be a part of it. Then the spam went through. This is one type of victim.

The next question, which we also have in other Internet cases, for example, fraudulent website cases, auction fraud cases, etc., is:

> "Okay, who is the victim?" How do we determine who the real victim is in a case like this?

The victims could come from lots of different places. They could be the individuals who purchased the products, which would be the quack medical products that don't actually work, and so they are out money. In this type of scheme there are going to be a lot of people who fall into this category. How do we determine who they all are?

That's one way of looking at it, from a consumer fraud angle. The other way of looking at it is [that] every single person who received the spam [is a victim]. That's getting to the point of being impossible to

> keep track of since this spam was going out at rates in the millions of emails.
>
> So, from this angle you are talking literally millions of possible victims. Another type of victim would be the ISP's, your Internet service providers who may have been in some way or another damaged by the fact that they received all this spam.
>
> So, it was a very difficult question in terms of who the victim is in a case like this. Because, at least in the federal system, and I'm sure it's true in states too, there's a very serious regime of laws regarding victim/witness relations [among] the government and the victims that involve things like notification.
>
> If you're going to take a case and say that as part of the case you have several million victims, does that mean that you're going to take the responsibility of contacting all these victims, telling them what court dates there are, making sure they have an opportunity to talk to the court at sentencing?
>
> So, it becomes very, very difficult. In our case the way we dealt with it was almost by punting and saying, "we're not really going to consider all of these people that received the spam or even purchased the product as being the victims" because we did not have quantifiable financial losses.
>
> Instead, rather than trying to accumulate the loss amount for sentencing purposes through that method, we simply looked at how much money was [the defendant] actually making because the federal sentencing guidelines allow us to use "gain" when loss is hard to determine. So that was kind of how we dealt with it. I just wanted to give you that as an example of a case, and try to address that.

In addition to the value of task forces, another area that there was unanimous consensus among the panelists was the advantages that come with cross-designating a state assistant attorney general as a Special Assistant U.S. Attorney. PRO-

FESSOR CORBETT expanded:

> [Assistant attorneys general] should consider getting Special Assistant U.S. Attorney status. It is something that can really put you in a unique position to be able to make the case. If you've got the monetary threshold met and you're working with a task force like so many people have talked about already, and you've also got the Special Assistant U.S. Attorney status, which is something you get by working with the U.S. Attorney in your federal district, you're in a position where you can take the case.
>
> You can be the one that takes it into federal court. Or, you can take it into state court. Whichever jurisdiction works the best, consistent with what you, as part of a task force working with the federal or state or local officers, have concluded is the best way to go.

As a practical matter in obtaining such special status, TERRY BERG observed that it should be for a specific case or series of cases and not just a general designation. He added: "If you're going to do that, try to make sure that you have an [actual] case that you want the person to work on."

TOM SADAKA provided a final example of the effect that different jurisdictions or districts can have even within the federal system:

> Of course the real fun is when you start ending up dealing with multiple districts. We had an identity theft ring that we chased up into Georgia [from Florida] and made the arrests in Georgia. The case was handled by federal prosecutors in Georgia. One brother pled out to five years in prison with the agreement that he testified against the other.
>
> The other was successful in getting his case transferred to the Southern District of Florida, [where it was] promptly dismissed it because it was below their million [dollar] threshold.

A final comment on effectively dealing with large numbers of victims and the inevitability of multiple jurisdictions was offered by TODD LAWSON who expanded on how large numbers of victims create notification problems:

> Most of our big victim cases, when it gets over into the something hundred range, we haven't even necessarily been able to contact them all. Usually in those circumstances we're finding the victim's information in the possession of the defendant after execution of the search warrant.

Only in the rare eBay case do we have all the victims talking to us. Even then, by the time we do get around to arresting the guy, 30% of those people have moved on or don't want to deal with us anymore because we've taken too long. In a number of our cases, the first contact with the victim is when we send the victim notification letter to say, "Hi, you're a victim."

QUESTION 3:

What role does the characteristics of Internet victims or their experiences play in the decision whether to prosecute?

The panel examined the characteristics of the crime and the particular victim or victims when "triaging" a case and making the decision whether or not to proceed. TERRY BERG stated the question this way: "What kinds of cases involving what types of victims should get priority?"

Some of the characteristics discussed prior to the panel were:

- seriousness of crime/victimization;
- ease of victim identification;
- chance of recidivism with the same victim (e.g., incest, etc.);
- age of victim;
- previous instances of victimization;
- ability of victim to testify adequately;

- credibility/perceived character of victim;
- whether victim is a "persistent" victim (with regards to past claims);
- trauma to victim from testifying in court;
- "politically-connected" victims; and
- existing or anticipated press coverage of victimization/victim.

One of the most prominent characteristics that emerged as being relevant in the decision to prosecute is whether crime involves a "real child victim." "For instance, in your child exploitation cases, try to focus, if possible, on those cases involving real child victims, whether being exploited sexually or just simply being the subject of child pornographic pictures."[6]

The panel considered not just characteristics in the affirmative, but also in the negative, in terms of "red flags" that might cause hesitation on the part of a prosecutor to accept or pursue a particular case. One such "red flag" identified initially by TODD LAWSON is where the victims have themselves retained legal counsel: "I'll tell you the number one thing that I do not like to see are lawyers. If victims have lawyers, I immediately step back. If defendants have lawyers, well, that I've come to expect."

This "red flag" often occurs in cases involving corporate victims, as TODD LAWSON continued:

> I have had one occasion, where it was an organized crime kind of thing where the defendants had a business front. The victims were so numerous that one of them was a lawyer and the lawyer has whipped up the other victims into fervor and they have started to talk about going class action lawsuit.
>
> Then somebody says, "Hey wait. Let's call the criminal attorneys." I say, "No, you go run with that. You take care of that on your own." If the victims have

---

[6] *See supra* note 3 (paraphrased version of conversation among Panelists and Moderator).

> enough money to hire their own lawyers, they probably have enough money to seek their own civil recourse. So, we generally step away from those [cases].

PROFESSOR CORBETT continued on this topic, relating his experiences that crossed-over between his time with the attorney general's office and his time as a law professor. Specifically, Patrick Corbett articulated the importance of gauging the victim's motivation in turning to law enforcement:

> Two quick stories related to the issue of dealing with the corporate victim. When I worked for the attorney general's office, we'd receive calls like this and since I've been a professor, I've received calls from attorneys on behalf of businesses.
>
> Generally, the claim is that this former employee hacked into the computer system and we're bringing the case to you. We're representing the corporation and we're bringing the case to you to go ahead and prosecute it for us.
>
> Well, I still remember vividly having a lengthy discussion with this attorney from the Detroit area working for [a] silk stocking firm. He's going on and on with the IT person there talking about how bad this was, and this employee was really out of control.
>
> Fortunately, we took some time to think about it; because it turned out they were involved in a serious labor dispute. The employee sued the corporation. He ended up winning. The corporation ended up paying out something like $500,000.00 in a suit. You have to be really leery of that.
>
> Just to give you another story, I'll periodically get calls from corporate attorneys and criminal defense attorneys at the law school. I had this one guy calling up and he's representing this business.
>
> He says, "So, I'm wondering if you can help me figure out what statute would be applicable, and which law enforcement entity I should call to get this case pursued?" So, I'm going through it with him. I'm

> thinking, "Well, it sounds like you might have some problems with your case with regards to whether or not the access was wholly unauthorized. That's always a big barrier. Do you have employment agreements or acceptable use policies, things like that? That's what law enforcement is going to be asking you about."
>
> We talked for about a half hour, forty-five minutes, and got to the point where I said to him: "I'm a little worried. I just have to ask you this question. Why is it that you want to contact law enforcement?" He told me directly that he's looking to gain a civil advantage in his lawsuit. Came right out and told me that. You always kind of assume it but this guy told me flat out.
>
> That's what it boils down to. If you think you're being contacted for the civil advantage of the case, or a corporate-type case, that's the caveat. It's not just that you're being contacted by a lawyer, it's that you're being contacted for the purpose of them utilizing your office to gain a civil advantage.

TOM SADAKA emphasized that the fact there is a lawyer involved, or a lawyer contacting law enforcement for assistance, does not necessarily mean that the motivation is to gain advantage in a civil case. He shared another experience:

> I'm working with a company right now. We found a whole load of child pornography on their system. I'm going to call a prosecutor on that case and I'm not trying to gain any civil advantage.
>
> I want the crap off the system. It's contraband *per se*. There are no exemptions or exceptions under the law. I need law enforcement to come in and get that stuff off the system. So, I'm not trying to gain a civil advantage. So, don't just close the door because you have a lawyer who is representing a company coming in. Look beyond to see what the motivation is.
>
> Cases where the victim may be politically connect-

> ed, in the public eye, or high profile for some other reason can affect the initial decision to prosecute. Prosecutors' offices are led by an elected official and are dependant (at least in part) on the legislature for appropriate statutes and funding.

As such, certain pragmatic concerns are always present. TODD LAWSON suggested this topic and started the discussion:

> For example, when we have state legislators who call, we try to give them the function of constituent service. It helps them to understand the problems faced by regular constituents. I mean, a state legislator told us earlier this year that he doesn't understand identity theft because he doesn't own a credit card.
>
> So, there's a fundamental level with some politicians and some people who are higher profile that you do have to take their complaints sometimes just to work them through the process, even if it isn't necessarily your biggest case.
>
> Jack [Christin, of eBay, Inc.] knows. I've been bugging him about a politician who lost $4,000.00 on eBay. But, it's not a big case. It's probably never going to be a big case because our bad guy is in Chicago and he's pretty good about hiding himself. But, it does help to kind of walk them through the process of what help a victim can get, it helps us and it helps them understand better.
>
> The other thing we do [in relation to high-profile and public cases] is we just watch the papers and watch for cases where there is an Arizona angle or a place where we can step in and help. It just makes your agency more responsive to the needs of the public and kind of helps you out in the court of public opinion, which helps you at the legislature.
>
> So, they're not the biggest cases. They're not your most important cases. But, sometimes they're the ones

that get you the most mileage in other ways.

PROFESSOR CORBETT offered insight into a situation where the perception that certain crimes were reaching "epidemic" proportions made the entire community a type of victim and, because of this exposure and publicity, the decision to prosecute was affected:

> I just have a quick comment on a case that occurred in Michigan that I think fits with this concern [very] well. In this case, there was a kid in Michigan who was communicating with a kid in Washington state through a chat room. The chat discussions revealed that the Michigan student planned on doing some bad things. It turned out that the kid in Michigan had a treasure trove of firearms and guns. Law enforcement did a search and ended up arresting the father and the son. This case was a pretty big deal in the area of Macomb County, Michigan.
>
> This same school district [Chippewa Valley School District] has had some more problems related to stalking and problems with teen use on the Internet. A seventh-grade, 13-year-old using [AOL's] [I]nstant [M]essenger (IM) to communicate with her friends and some people that go to the school, had basically threatened to blow up the school.
>
> For these threats, she was prosecuted by the Macomb County prosecutor's office using a 20-year [sentence] anti-terrorism felony that was passed by the Michigan legislature in 2002, shortly after 9/11. They're doing this for the deterrent effect, the fact that there's this huge amount of community interest in it. It has, I think, had some significant effect, because a lot of different parents and educators that I have spoken with have heard about this case. They talked to their students and kids about it. So, there is some value in doing it from that type of perspective.
>
> Who's the victim here? Well, it's the school dis-

> trict. It's the community as a broader matter. So, there's some value in taking a case like that. Sometimes it is purely for the deterrent effect. We can, of course, question whether or not a 12-year-old sending instant messages is the right defendant for an anti-terrorism law and there is some head scratching that goes on there. But, that being said, clearly it's serving a function.

TERRY BERG expanded on this idea related to the public's perception that certain crimes (i.e., Internet ID-theft, school shootings, child pornography, etc.) have "suddenly become something extremely serious or of an epidemic proportion." He added:

> The question relates to when you have a case or a series of cases that in the perception of the public have now suddenly become something extremely serious or of an epidemic proportion.
>
> Whether it's in the case where the minor has used the Internet to threaten a Columbine-type of act in a high school or a number of smaller incidents that we've had in my state where students have expressed threats, even in one case on a bathroom [wall] which resulted in very immediate and "robust" law enforcement response in terms of charges against the minors who were involved.
>
> I think it is a combination of a lot of pressures that we're talking about here. You have the question of the vulnerable victim—these are children that are in a school situation. Then you also have the public perception of danger associated with any Columbine-type of crime which, obviously, law enforcement and [the] community wants to make certain never happens again.
>
> I don't really know the answer to a question like that. We had some questions from the press to our office about [one of the school threat cases]. I could tell

> from the question that the person asking [was] fishing for a response like: "Well that's an overreaction. We don't necessarily . . . ." Of course, I was never going to say anything like that, because frankly I can't say that it was an overreaction [where] you have a situation where there is an actual threat of attack on school children.
>
> Of course, law enforcement has to take it seriously and respond. But, it's a difficult juggling act. Before Columbine, it is likely that many of these cases would have been treated with only an interview to determine whether there was an actual threat. In many cases, law enforcement would not have been directly involved, instead it would have been handled administratively and internally at the school.

Collectively, from the comments above (and some made by the audience) it became clear that, in many cases, prosecutors felt different types of pressures based on politics, public or media interest, or other factors, which could, in turn, influence the decision to prosecute. In some instances, where the community expressed interest or an expectation in a certain matter, the community as a whole becomes a distinct Internet victim that warrants consideration.

Of course, pragmatic concerns will, in many instances, have to yield to ethical or prosecutorial duties when deciding whether to prosecute. TOM SADAKA stated:

> That's fine as long as it doesn't then impede upon your ethical obligations to have reasonable certainty of convictions when you file the case. There are a number of times where the political pressures try to get you to file on a case that you know you can't prove. Or at least you can't prove it the way that it is charged. That's really where the separation is. You can accept the pressure, but stand by your ethical obligations.

QUESTION 4:

What are the policies and procedures related to case acceptance or denial?

One question that was posed to the panel related to policies and procedures related to the decision to prosecute. The moderator posed the question this way:

> We've pretty much been talking about all these things from a very subjective, discretionary point of view. But, fairly quickly, what mechanics, policies, and procedures are there relevant to these triage or charging decisions? And then what role does the victim play? Does the victim play enough of a role or too much of a role from your experience?

One procedural consideration that was mentioned by TODD LAWSON was whether or not he has to list a particular victim:

> I've already referenced one tool that I use in terms of mechanics of the decision, [which] is I like counts where I don't have to name the victims. I like the ones that give me expandability where I can have five people testify in support of it, or, in theory I could have 228 testify in support of it.
>
> So, sometimes it's the charge you select, and the requirement that the charge identify a particular victim in its text. Whereas, there are certain advantages if you can just attach a victim to a group count.

TERRY BERG provided an in-depth examination of this question. While his answer primarily addressed his opinions in the context of the federal system, the interesting hypothetical has broader application and is helpful to state prosecutors as well:

> There are also cases where you have a victim who

presents problems. The troubled teen victim in your child exploitation cases would be an example. For instance, a case where the scenario is that the defendant is an individual who's himself close to being a minor—let's say around 19 years old—is chatting with a minor female on the Internet in a sexually inappropriate manner.

Let's say the defendant has a very dark personality on the Internet. He's posing as a person who does contract murders and he's just an awful person. This teenager victim is actually chatting about possibly having this person kill her parents. So, this is obviously a very troubled teen.

As the chat continues, this develops and it becomes your typical solicitation situation and the defendant solicits the minor to send pornographic pictures of herself, which she does and gets her friend to do it as well. In this example, you can see that you have a very troubled person who is also a victim.

So, then the question becomes: "What's the proper thing to do. How do you deal with a case like that? What's the proper way to charge it?" For example, in the federal system there are mandatory minimums that apply in child exploitation cases. For production of child exploited material or child pornography, you can get between fifteen years as the minimum and thirty years [as the] maximum.

So, that's a very big hit. Here, you're talking about a defendant who is close to being a minor himself—19 years of age. You have a production situation, which is arguably not coerced at all because of the nature of the troubled teen and the nature of proof in the case.

So, the question becomes: "Do you go for that?" "Do you give the maximum charge?" Or, "do you go to a lesser charge?" For instance, instead of being production of child pornography the defendant could be charged with transmission or receipt of child pornography, which has less severe penalties.

> Anyway, I'm just bringing all that up to say that this is how I think victims come into play in the charging decision. I've mentioned some of the procedures we go through. In my office they would be all those facts I've just laid out in an attempt to determine whether or not you would give the person an opportunity to plead guilty to a lesser charge.

QUESTION 5:
What are the challenges in dealing with law enforcement in Internet victimization cases?

Another subject discussed was the challenges in working with law enforcement agencies in the context of an Internet crime case. It appears that many of the problems that arise are related to jurisdiction; the willingness to take the initial police report when it is unlikely any action will be taken by the reporting department; and, pragmatic issues that arise with crime statistics and law enforcement's general resistance to change.

Law enforcement agencies, for a variety of reasons are reluctant to take police reports in Internet victimization cases. In response, the Arizona, Attorney General's Office prompted the legislature to change the "I.D. theft statute to say that the [police] report can be taken where the victim lived or where the perpetrator was" according to TODD LAWSON. However, the police departments lobbied the legislature to change the law back to its original form. The Arizona Attorney General's Office again worked with the legislature and the law was changed back, again, to allow for the report to be taken where either the victim or the perpetrator lives.

Why would police departments not want to take police reports? Several reasons were discussed. The first goes back to budget. Police departments are concerned that because of budgetary restraints, they will not be able to do anything for the victim.

TODD LAWSON expanded on the situation in Arizona, exemplifying on this difference of opinion or priority:

> Yes, we went round and round with [law enforcement] on that. The basic underlying principle of it was you give a guy who calls up and says, "Hey, somebody just stole a bike from my open garage" a report, why not give the guy who calls up and says, "Hey, I just had my identity stolen." Prosecutors believe that this is very important because of how many of these cases start with a single report. The response of the police is: "Well, we can't investigate this stuff. We don't have the money to do that."
>
> One cause of this tension between prosecutors and police appears to be the expectations placed on the police if they take a report. The question arises: do you have to do a follow-up investigation on every police report? Several audience members provided information about states that passed legislation stating that, though the police departments should take the report, they do not necessarily have to conduct a follow-up investigation.

TOM SADAKA stated that a specific statute was likely unnecessary because law enforcement is generally not required to investigate every report:

> The irony, though, is that it is underwritten in every criminal code that there is no obligation, maybe with the exception of child abuse, on the part of law enforcement to conduct any investigation. So why, just because you've created jurisdictional ability for them to take the report, or really just a clarification, because the jurisdiction really existed regardless, why do they now feel that because it says they can investigate that in this instance they are compelled to investigate? These departments have always had the ability to triage everything that came in anyway.

A second reason for police reluctance is that certain cyber crimes because of multiple jurisdictions and other factors do not fit into the normal model for law enforcement statistics. An audience member relayed the following story related to how the manner in which clearances are indicative of job performance can make this type of crime less than desirable from a police point of view:

> When this identity theft issue came up initially, the police chief was very interested in it and encouraged it and everything. So we were rolling it out and getting this particular agency involved. When the first shift lieutenant realized that his shift would have to take this type of report, he became furious about it. The reason is that they don't get a clearance right away. His shift ends up taking the bulk of the reports but he's not getting any additional manpower to pursue the reports and, in many cases, this isn't the type of crime that the agency would be able to investigate as it might only be the victim that lives in the jurisdiction, not the perpetrator. So, in time, his clearance rate goes down. He looks bad and he's demoted.

TERRY BERG commented on this point (to the general agreement of the audience) that it is "an administrative issue. They could create some kind of code on an identity theft report that doesn't factor into the clearance rating. That's purely an internal administrative issue and shouldn't factor in." PATRICK CORBETT added that, in many cases, the actions of the legislature created problems because of increased expectations on law enforcement without any additional resources:

> It gets back to what the legislature's doing. They are imposing more and more new opportunities or requirements on various law enforcement entities, but generally not supporting these entities with any kind of increased funding.

PANEL DISCUSSION II

PREPARING THE CASE AFTER THE DECISION TO PROSECUTE HAS BEEN MADE

INTRODUCTION

Our second panel discussed the elements of preparing a case after the decision to prosecute has been affirmatively made. Again, taking into account the victim to whatever degree necessary or desirable, we are now looking down the road towards trial. Obviously, with the group in attendance, we did not need to talk about the specific steps of trial preparation generally; rather, we wanted to discuss the consideration, involvement, or relevance of the Internet victim to each of these steps.

Marc Harold[1]

---

[1] Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.

PANELISTS:[2]

- Richard Hamp, Assistant Attorney General, Office of the Attorney General of Utah
- Jean Smith Vaughan, Special Assistant Attorney General, Chief, Cyber Crime Division, Office of the Attorney General of Mississippi
- Kelly Carter, Assistant Attorney General, Office of the Attorney General of Michigan

QUESTIONS FOR PANEL:

1. What type of "special" discovery takes place when dealing with an Internet victim, if any at all?
2. What input does or should an Internet victim have in the plea bargain negotiation process?
3. What are the difficulties and/or challenges in assessing victim credibility in Internet cases, and is there anything unique about Internet cases in this context?
4. How do you maintain communication with the victim during the trial preparation process generally, and, more specifically, how do you "preserve" the victim during trial preparation?

QUESTION 1

What type of "special" discovery takes place when dealing with an Internet victim, if any at all?

RICHARD HAMP began by discussing the manner in which discovery can be unique in Internet victimization cases:

> When I first considered "What is different about an Internet victim?" my first thought was that it's

---

[2] It should be made clear, at the outset, that the statements and opinions offered by the panelists and moderator are solely their own and are not offered on behalf of any organization or agency.

> really not that different from any other victim, except their location may be a bit removed from my office. But then it dawned on me that there can be a huge difference in an Internet victim, particularly when you're talking about a phishing scheme or something that now, instead of one victim of that crime, you have 500 or 1,000 victims of a particular crime. So, when you are looking at discovery, if you're showing a phishing scam that went out to all 500 victims, now do you need to manage discovery of 500 different victims' computers through several different states as part of your case? And, if so, how do you go about managing all that? How do you keep your lines of evidence intact, your evidence chain? So this can be a huge management problem that you start with up front. So it's something you need to think through very carefully in terms of your charging decisions as to not only how you charge the case, but also your case management decisions after you have charged the case and are looking to move the case through the trial process.

KELLY CARTER continued and particularly discussed the value of organized, systematic data collection and recording when attempting to manage such large-scale discovery:

> Although I'm now doing more child porn and predator cases than in the past, when I was dealing more frequently with the more large-scale auction fraud cases, or cases of that nature, I found that the U.S. Postal Inspector Agents have been very helpful. One of the things that is most helpful in preparing a case is the systematic way in which they approach the evidence. When considering discovery in a case like that, I rely on this very organized agent to communicate with the victims and gather the same types of evidence from the victims. For example, "What was the date of the transaction?," "How much was the

> loss?," "Do you have credit card records to back it up?" Compiling all of this information systematically and converting all of the information to a spreadsheet is very important. So it's the actual agent that has all the backing documentation. For my purposes as a prosecutor, I've got the spreadsheet which puts everything in a nice package for me so that when I'm talking about my victims I can either organize the information according to the amount of loss or distance or whatever the case may be. So, when we're talking Internet victimization cases, which are often cases with a large number of victims, the important thing as far as discovery goes is the systematic nature in which the information gathering and recording is conducted and how that information is all kept together and available for my use as a prosecutor.

JEAN SMITH VAUGHAN discussed the use of business records when conducting discovery in an Internet victimization case:

> Also, a good deal of the information Kelly discussed might be available as a business record, like through Yahoo! or PayPal, especially if it is kept in the ordinary course of business. This way, you will have all the credit card transactions for example. In the context of child pornography, especially when attempting to show that it is a real child, we work closely with the National Center for Missing and Exploited Children ["NCMEC"]. Once we have the images we need and we think we're going to charge, we send the images through the Postal Inspector, which then goes through a certain process which allows us to maintain the chain of custody through law enforcement. This way, NCMEC can verify for us that these are indeed children that have been identified and who are in a known set of pictures. They are identifiable, and thus, it can be proven that the image

is of a real child.

KELLY CARTER commented:

> I think in addition to NCMEC files, I believe that the FBI and U.S. Customs also have collections of known child pornography series or known image. So if you find yourself dealing with a child pornography case and you are at that step of attempting to prove that they are, in fact, real children in the images you have, those are other good resources.

JEAN SMITH VAUGHAN continued and discussed some of the difficulties encountered when you are not able to identify a child through these means, for instance where you get the pictures digitally:

> Of course, there are kids you just can't identify. For example, there are kids on a picture that you've gotten digitally. My office is having a lot of cases involving homemade child pornography now. For instance, I have a person hopefully we'll get to plea tomorrow, who's a seventeen-year-old who has made his own child pornography with his nephews. It was an all summer long affair. He had a web-cam, videotaped it, and saved the videotape. He got the nephews to act out in all kinds of sexually explicit poses, masturbating, and on and on. He saved it and then transmitted it to his buddies in chat rooms. I'm also afraid I'm seeing younger and younger perpetrators. So, when you get into discovery in these cases, it is the victim who is in-state. We try and go and have the victim interviewed at the Child Advocacy Center. As with any child abuse case, you don't want the victim's name out in the public, and you kind of want to shield it in discovery with the defendant.

An audience member commented on the possibility of

Confrontation Clause problems that might arise when conducting discovery in Internet victimization cases. Specifically, members of the audience mentioned the U.S. Supreme Court's ruling in *Crawford v. Washington*.[3]

KELLY CARTER stated:

> I've actually got that in a couple of weeks. I've got a child porn case, and the pictures are from the "Helen and Gavin" series. So I have the records, and I've got on the witness list both the NCMEC representatives as well as Constable—what's-his-face from wherever in Wales, but I've also got that cost-of-prosecution hammer that I've got going on too. So I've put that on my witness list and let defense counsel know that "I'm still prepared to book the ticket for the Constable from Wales, and you're more than welcome to pay for that if you want, or you can stipulate that these are known children from a known series." You can remind defense counsel that, since these images are from an identified series, "I can always cross-examine your expert witness on the knowledge of who these kids are." Of course, I would still be prepared to bring in the Constable from Wales to identify the victim if it is necessary.

JEAN SMITH VAUGHAN continued:

> I think you can also bring in the people from NCMEC, and they will come and identify that the pictures are from a series that have been collected for the purposes of prosecuting these crimes. This might not completely alleviate your *Crawford* problem, but it certainly does help in terms of pleading and in preparing for trial with your defendant.

---

[3] 541 U.S. 36 (2004).

RICHARD HAMP shared his thoughts on issues related to the chain of custody:

> One thing that Utah has, at least in our case law, that does help, not necessarily with *Crawford* but with chain of custody, is we have a case called *State v. Wynia.*[4] If you're talking about a tangible item that can't be easily altered, something other than drugs, paperwork, or a gun or something like that, if you do have a violation in the chain of custody, it now becomes the defense's burden, rather than the prosecution's, to prove that the evidence was somehow altered or tampered with.

QUESTION 2

What input does or should an Internet victim have in the plea bargain negotiation process?

RICHARD HAMP:

> Utah is kind of unique in this particular realm. We've got statutory authority in the form of a Victim's Bill of Rights, which requires that we get victim input on a plea. As a matter of fact, we had one case that was reversed because the prosecutor didn't consult with the victim beforehand.
>
> It's kind of an interesting area. It requires you to get input, but then it does not require that you have to follow what the victim says in terms of a plea—but you do have to at least get that input from the victim prior to the plea. Clearly, when the drafters of that statute put it together, we were not dealing with these huge Internet crimes that involve hundreds of

---

[4] 754 P.2d 667 (Utah Ct. App. 1988).

> victims. At the time, we were talking about homicides and child sexual abuse that maybe involved one or two or five people, so, at the time, it was a great idea. But now, at least in its practical application, it is quite hampering on a big Internet case to have to get that type of input prior to every plea. Fortunately, we don't necessarily have to follow the input, but the victim does have the right to speak at sentencing. I've had them stand up, on occasion, and they strangely object to what the prosecutor has done with the case.
>
> For example, I had a death penalty case a few years back where I had multiple victims of a serial killer. Some of the families were kind of in the middle and didn't know if they wanted the death penalty or not. I had one family that was entirely opposed to the death penalty and one family who wanted to execute the guy themselves. So, of course, I'm trying to balance all of this in coming to a decision on whether or not to seek the death penalty, which would determine how I would argue it in court. The face of prosecution has changed within the last decade with the victim's rights statutes. I think it's good for the victims, but it has certainly made the prosecutor's job much more difficult.

JEAN SMITH VAUGHAN expanded on the issue of victim's rights:

> In my perspective, how importantly I consider the victim's input as far as a plea, I think it is in direct proportion to how personal or how egregious the victimization has been. Clearly, in the $50.00 auction fraud situation, I'm going to put my own considerations first as far as how many cases I've got, which ones I want to plea, which ones I don't want to take to trial. These types of practical considerations are certainly going to impact my consideration of the

victim's input. Of course, I'm still going to ask for the victim's input in those cases because we have an obligation to do that, but as to how much consideration I'm going to give that input, it may not be as great in those cases as opposed to the types of cases where I have a real child victim in a child pornography case. Recently, I've had more cases where I've had adult victims. For example, I had a recent case where the victim was, now, a twenty-seven-year-old woman who had been victimized when she was sixteen. Her role in that case was vital. I would have taken what she said and let it control how I was going to handle the case. Clearly, her level of victimization in that case was, to me, more important than the impact it was going to have on my docket or whether I wanted to try it or not. So, as far as I'm concerned, that's generally the sort of consideration that I'll give the victim with regard to whether I'm going to plead a case or not and where the victim is coming from on it.

Further, I had a case this past summer where it was an emergency room physician, a sixty-year-old who had previously been a pediatrician. Perhaps something had occurred [in his past] that [as a result of which] he was asked to leave pediatric medicine. He became an emergency room doctor. This doctor lives in a different state, but he started to visit his granddaughter on a regular basis. He seemed to prefer one of the two granddaughters over the other. He would read her stories, bring her toys, stuffed animals, this type of thing. I think that the grandmother was very complicit in this instance—I think she knew about the abuse but did nothing about it. He was prosecuted for fondling his granddaughter. In this particular case, the family played a tremendous role in determining what would happen to this particular guy. He was a doctor. The son, who was the father of

> the victim, was also a doctor. It was essentially a rift in the family, where the grandfather and the grandmother will no longer see those grandchildren, because they split. The family dynamics [were such that there were accusations that] it was all the fault of the mother or the wife of the father—allegations were made that she'd just made it all up. Not really, the little girl was very articulate and was prepared to testify at trial about the acts of the grandfather.
>
> In this case, this particular family did not want the grandfather, the E.R. physician, to do any jail time. That was more than they could comprehend—more than they could handle at that point in time. So they asked the judge about it and made a plea offer to him. So the guy gets convicted but no jail time. He is a registered sex offender in Mississippi and Texas. When he spoke to the judge, there was actually no remorse there. The remorse was that his wife would no longer get to see the grandchildren, but you know how defendants are sometimes.
>
> It's like they're pleading guilty, but it's like, "Are you guilty because you are really guilty?" Well, he said, "Yes," but his body language and everything else he said was, "No, I'm not taking responsibility for this." So, in this instance, I didn't feel comfortable with that. The judge looked at him very carefully and said, "[I'm] going to watch [you] like a hawk." [The judge] thinks [the grandfather] will be a repeat offender—he's not just someone who woke up at the age of sixty and started abusing his granddaughter. So this is one of those cases that [is] kind of bittersweet—the guy got convicted, but he didn't go to jail. The family just couldn't handle that.

An audience question touched on the issue of the effectiveness and helpfulness of victim-witness coordinators. RICH-

ARD HAMP commented:

> In Utah, we have victim-witness coordinators that help out. This was something that I was going to bring up yesterday during one of the presentations, specifically, "How do you explain to the parents of the victim what happened to their kids?" We had a very good suggestion about focusing on what the perpetrator did and not anything that the victim did. The other comment I have is that dealing with distraught victims is, unfortunately, not my expertise. There's no coursework that I've ever been offered or taken that tells me how to deal with victims. So, I've kind of just had to learn it as I go throughout my career. Sometimes I think I do it well, other times I don't think that I handle it well at all. But I know of someone who does it very well, and that's my victim-witness coordinator who has had that type of training. So, in this type of case, I try to get the victim-witness coordinator involved as early as possible to help out with that angle of the case. That way, I don't have to worry about bringing a skill set to the table that I really don't have.

At this point, the discussion shifted from audience discussion to what, if anything, makes an Internet victim unique in comparison to other types of victims and the effect that this might have on the overall analysis about victims and plea bargains in the Internet victimization context. KELLY CARTER opened this part of the discussion:

> To some extent, it again depends on the type of crime that's committed on the Internet. For example, I unfortunately had a child porn case where it was the picture of a known victim that was put up on the Internet. In that case, obviously, the humiliation of that known victim and everybody in her community knowing that those pictures were there and seeing

those pictures, that intensifies her victimization in that type of Internet case. It's not just a situation where some pictures are taken and handed around a locker room. They were actually posted on the Internet, and everybody in her school knew that they were there, and everybody saw them. So, I think, in that sense the Internet victim is, in some ways, more vulnerable, just because of the vast exposure that the Internet provides, certainly in the sense of child situations. In some circumstances, the victim of an Internet crime can feel even more duped than in a typical case. For example, we have the Nigerian situation, and anybody who has fallen for the Nigerian scam letter probably feels a little more foolish than the average fraud victim because of how widespread and obvious that particular scam was. So the notoriety and, again, the widespread nature of some of the crimes make the Internet victimization more intense.

JEAN SMITH VAUGHAN continued:

Kelly has hit on something, and that's the continued victimization of a particular person, because once the picture is out there, it's accessible for a long period of time. One case that comes to mind is where two college students were killed by a man. He was on trial for it. It was a death penalty case. There were some problems with the case, and so there was going to be a retrial. In the meantime, someone with some interest went to the clerk of court and checked out the record, got the autopsy photos, and posted them on his website saying, "This is what happens (in this particular type of crime)," or something like that. He was anti-death penalty, anti-black on white crime, and there were racial overtones posted on the website. Another jury was going to be sworn in quite quickly after this happened, and we were able to get the pictures sealed and put back into the court docu-

> ments. But, again, it's that same type of thing, like the Dale Earnhardt autopsy photos and people who wanted to put those on the Internet, it's a type of victimization, but it is a continuing victimization.

Next, the Panel discussed the very real sense of invasion of privacy and loss of trust that Internet victims experience. RICHARD HAMP commented:

> There's two points to remember in this. The first is, and I think it is on the FTC website, there's a study that came out [saying] that victims of particular identify theft and that type of financial crime feel a lot of the same feelings that rape victims do, particularly with regard to the invasion into the victims' personal space of their financial identity. They feel the same shame and remorse and depression. There have been studies that show where they [a victim and his or her spouse] have ended up being divorced as a result of the victimization. Lost jobs. I mean, this is a crime that really does affect the victim much more than just in the pocketbook.
>
> Plus, the system self-perpetrates the crime again and again on the victim, particularly when you're looking at the credit score. The information from the crime spree keeps showing up over and over and revictimizing the victim. The victim will go through a year or two or three to get it off, only to then have it put back on by another reporter in the credit bureau system that's picked it up from another source and then puts it back against the credit rating again. That's why we say that identity theft is the crime that keeps on giving.

QUESTION 3

What are the difficulties and/or challenges in assessing victim credibility in Internet cases, and is there anything unique *about Internet cases in this context?*

KELLY CARTER spoke on this question first:

> Generally, when it comes to Internet cases, I think sometimes you have the possibility of your victim seeming more sympathetic in the sense that people who have been on the Internet and experienced certain things may be slightly more sympathetic to your victim in the sense that they are thinking, "Okay, well, there but for the grace of God, go I. That could have been me—I've been in that situation, and that could have easily happened to me," because there are so many people who are putting themselves out there and in potential jeopardy. So, it's possible that, depending on the circumstances, your victim may be more sympathetic and may be a slightly more credible witness; however, I think that it also cuts the other way as well. Sometimes people might think, "Yeah, but that wasn't me because I took the steps to make sure it didn't happen to me. I made sure that I didn't put my picture on the Internet so that someone else could put it out there and post it." And, I think in that sense, it could make your victim's credibility more of a problem in that you have that, "Why did you do that?" sort of mentality where people ask, "How could you not consider that as being an issue?" In this type of situation, your victim might seem potentially less sympathetic. Unfortunately, I think that's probably going to depend on the circumstances of the case and whether it's a child porn case or an auction fraud case, whether it is older victims, younger victims, or middle-aged victims—all of that will come into play. I think being an Internet victim is going to weigh both ways on the credibility of your victims, potentially.

JEAN SMITH VAUGHAN expanded on this topic and offered an example:

> I had one case in particular. It involved a lawyer who was a victim of a vicious email. It was sent to all of his colleagues, and it damaged his reputation. If truth be told, maybe his reputation was not so wonderful to begin with. It's kind of like, "How much do you want to protest (. . . *'the lady doeth protest too much.'*)?" He was satisfied, actually, with an apology from the person who sent the email and an acknowledgment [from that person] that he sent the email and a letter to the Bar refuting it. So we talked with the victim about, "How much do you want to say, this is not true?" [He adamantly responded,] "It's not true. It's not true." There was a question as to whether or not the continuing denials lent credibility to the content of the email.
>
> Then I have another case where the victim is a cheerleader. She's a twin. Her picture—the picture of the twin—was posted on the Internet in a sexually explicit pose. It was like good twin, bad twin. So the good twin, the one who is actually a cheerleader, was posed as the bad twin with the message, "I like sexually explicit things. This is what I want." As a result, the good twin lost her job as a cheerleader, so she suffered actual damages. There was also reputation damage as well as actual harm to her. But, in terms of sympathy from a jury, I'm not sure how much there would be. So the lesson is, you take your victims as you find them.

RICHARD HAMP discussed the value of meeting with the victim face-to-face and the difficulty in having this type of meeting, especially in Internet victimization cases that span over several jurisdictions:

> One thing I've found is, I like to bring the victims

into my office and do a face-to-face with them so that not only do they get to know me, but I get to know them, and I can kind of feel them out as to how good of a witness they will be. This also helps to gauge their credibility level. Oftentimes, when you have an Internet victim that is several states removed, you don't have this opportunity. I rely on a lot of visual clues that may not be apparent, or that you can't get over a phone or [from] some other way of communicating with the victim. So, in many Internet cases, it makes it a little bit harder for me sometimes to pick up on stuff that I would normally rely on before putting the victim in a court situation.

QUESTION 4

How do you maintain communication with the victim during the trial preparation process generally, and, more specifically, how do you "preserve" the victim during trial preparation?

JEAN SMITH VAUGHAN stated:

I have a traveler case. The girl was sixteen, and she was solicited on the Internet. The guy drove to Indiana, picked her up, brought her back to Mississippi, had sex with her, and said, "Well, there's nothing wrong with that. The age of consent is sixteen." But, under the statute, the relevant age for exploitation of the child age is eighteen. She didn't look like a child at age sixteen, and now she looks even sluttier. In this case, she really encouraged this guy, so that's going to be a big factor. They talked about what kind of sex they were going to have. She was running away from her grandparents and this, that, and the other. So she's not going to be the perfect witness. And, of course, he's making himself out to be the perfect angel who goes to work and to church and that kind of thing; however, in his spare time he's sending out pictures of his naked self to other under-

> age people, and so we have those chats as well. I also have some other victims. One is a meth-head and she's not very attractive either, but she's under the age of sixteen. So, as you can see, how they appear and how they dress can be a big factor of how they are viewed as victims.

KELLY CARTER continued and discussed the victim who's not there because the case is the result of a proactive law enforcement investigation where the victim was actually an undercover police officer:

> On the issue of trial preparation, my experience has been that as far as victims are concerned, if I've got a child pornography case, the victim is preserved as it happened through the actual images, so it isn't going to be an issue. It may have been a while ago, and the victim may look a lot different now, but, nonetheless, I don't think you lose that much sympathy for a victim when you're seeing the actual victimization. But one thing I would like to talk about is when the victim's not there. So, in the undercover cases when you've got the sort of traveler situation [involving a defendant] who had been talking with the undercover cop online, there really is no victim. Of course, the defendant is real quick to point out the fact that there is no victim in these cases. When I'm preparing for a trial in that sort of case, I'm jumping all over the fact [that] there was a fourteen-year-old—that the defendant thought there was a fourteen-year-old. So I'm going to refer not to the officer, but I'm going to refer to the name of the officer's persona. Regardless of the persona, I'm going to use the name that the officer was using when he was chatting as that fourteen-year-old. In a sense, what I'm going to do is create the victim that doesn't actually exist. Because, for all intents and purposes, this guy thought that there was a fourteen-year-old and that

> she was a real person. I think it has a lot of impact on a jury to tell them, "Okay, we got lucky here that there really wasn't a fourteen-year-old on the other end, and some girl was saved the trauma of this circumstance." So, in these cases, it's the non-victim victim that we're trying to create and preserve in that circumstance.
>
> Another point on the non-victim victim situation is that I am many times presented with people who consider themselves victims even though they are not victims under the Act. So, I will often hear from the wife or the family of the guy who shows up to meet the fourteen-year-old [and the wife will be] presenting herself as a victim—like, "What am I supposed to do, and how do I deal with this?" That's a difficult situation to deal with in that this is a person who truly has been victimized but not in our legal sense under the Act. So, in those circumstances, I will try and deal with that person. I also had a situation where the stepsister of this guy showed up during his sentencing and asked to be able to address the court to say that while she was young, he had in fact abused her. This was a traveler situation, and he had on several occasions been convicted of prior sex abuse, but this was a situation where there had never been a conviction based upon her testimony. She was just now showing up, and I had a difficult time dealing with defense counsel on that saying, "I know she's not a victim under the Act, but she wants to be able to address the court with regards to sentencing here." Some of the child sexual abuse situations do create victims that we don't necessarily anticipate, but that may present us with the situation where we have to deal with them as victims as well.

RICHARD HAMP closed the discussion on victims by providing a type of frame-work with which to consider different types of victims:

> One thing that I wanted to mention about victims, and we've kind of touched on this in our discussion, is I find that you've got about three main categories of victims. You've got the child sex victims who are very, very sympathetic victims. You've got your financial victims who, although real people, are really stupid people and it's kind of hard sometimes to sell them to a jury. Then you have the final category, which are corporations, large business victims. I find a lot of times when I've done jury trials with them, my juries are less sympathetic to the large corporations than they are to the other types of victims. So, I'm finding when I'm doing trial prep that I have to make the corporation seem to be more human by having the president of the corporation there or a good representative from the corporation in the courtroom on direct so that I can try and personalize the corporation. I've had cases where juries, although the evidence was clear, returned a verdict of not guilty simply because they didn't feel there was any victimization to the corporation, because they have plenty of money to cover the problem. And this poor little guy that was ripping them off, no big deal, blah, blah, blah. So it's something to watch out for when you're prepping these cases for trial and thinking about the likelihood of different outcomes. Maybe in those cases I could have done a better job of saying, "Look, this victim is no different than any other victim."

PROSECUTING THE INTERNET FRAUD CASE WITHOUT GOING BROKE

Patrick E. Corbett[*]

ABSTRACT

This Article contends that viable Internet fraud cases are not prosecuted as consistently as other Internet-related crimes. One reason involves the financial cost of bringing these types of cases to court. In general, Internet fraud cases involve multiple victims who have incurred only a small financial loss. Typically, the victims are from all over the United States and beyond. Hence, prosecuting the fraud case to the fullest extent involves use of witnesses from outside of the jurisdiction of the prosecuting authority. The cost of housing these witnesses and transporting them to the court where the crime is being prosecuted often exceeds the budget available for such an expense. Consequently, many prosecutors decline prosecution rather than incur the expense associated with a full prosecution. This Article explores various approaches to reduce the cost of prosecuting these crimes in order to ensure that Internet fraud cases are prosecuted rather than declined.

---

[*] Professor, Criminal Law and Procedure, Thomas M. Cooley Law School, Lansing, Michigan. This paper was commissioned by funds from the National Center for Justice and the Rule of Law at the University of Mississippi School of Law (National Center), which is supported by a grant from the Office of Justice Programs at the United States Department of Justice. The contents of this paper were presented at an April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center and the National Association of Attorneys General. Thanks to Tom Clancy, Director of the National Center, for the opportunity to write on the subject, and to Cooley Law School student, Lisa Esser, and Cooley Law School librarian, Tim Innes, for their research assistance.

I. INTRODUCTION

A. *A Hypothetical Internet Fraud Case*

Over the course of two months, investigators for the Attorney General's Office for the State of Chaos received fifteen complaints from consumers against a company by the name of Bargains Galore. Further investigation revealed that Bargains Galore used a post office box located in Cooley City, Chaos.

The consumer complaints alleged that Bargains Galore offered computer game packages for sale through Internet auction site eGads. After the auction concluded, the winning bidders were notified via email that they had won the computer game that had been bid upon. Winning bidders sent payment—typically between $150.00 and $250.00—through the U.S. mail or through an online payment service. According to the complainants, either no computer game was received or they received a dated game that was of no value to the complainant. The complainants advised they attempted to contact Bargains Galore on several occasions. On a few occasions, complainants were actually able to talk with a person; on these occasions, the complainant was assured that the computer game would arrive soon.

Of the original fifteen complainants, only one resided in the State of Chaos. The Chaos complainant lost $250.00 in his transaction with Bargains Galore. Further investigation by the Attorney General's Office revealed the existence of another thirty victims, none of whom resided in the State of Chaos. The total amount of loss for all forty-five victims amounted to approximately $20,000.00.

Fraud prosecutions in the State of Chaos are dependent upon proving a specific amount of loss. While a prosecutor is authorized to aggregate amounts of loss based upon multiple victims, the amount of loss must exceed $1000.00 to be punishable as a felony. In order to prove an amount of loss in excess of $1000.00, the prosecutor needs to gain the cooperation of at least seven to ten additional victims, the closest other victim residing in a state 500 miles away. The anticipated cost for travel, food and accommodations for these witnesses through trial: Over $10,000.00. The Prosecutor's response: Charge it as a one count misdemeanor involving the State of Chaos victim or decline the case.

B. The Correct Response? Are There Alternatives?

The limited budgets of most prosecutor offices prevent these cases from being fully prosecuted. How can the typical office justify spending $10,000.00 on witness expenses for a case that barely reaches a $20,000.00 amount of loss and that only involves a loss of $250.00 for a State of Chaos victim?

At the same time, there appears to be no lessening of Internet fraud cases. The Federal Trade Commission (FTC) recently reported that "Internet-related complaints accounted for 46% of all reported fraud complaints, with monetary losses of over $335 million and a median loss of $345."[1] Consumer complaints filed with the FTC reveal that fraud complaints have risen each of the last three years.[2] Are the fraudsters out there empowered to commit more crime due to an inadequate prosecutorial response? What can be done to maximize the likelihood that these Internet fraud cases will be prosecuted?

This article explores avenues for increasing the likelihood that Internet fraud cases will be prosecuted in a manner that maximizes the deterrent effect on existing and would-be fraudsters. Part II reviews methods for building the case at the outset, including exploring law enforcement databases and working with the private sector. Part III considers some alternatives for reducing the cost of a prosecution by, inter alia, simplifying the preliminary exam process. Part IV briefly explores the impact of *Blakely v. Washington*[3] and *United*

---

[1] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA: JANUARY-DECEMBER 2005 (2006), http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf. This report is based upon the consumer fraud and identity theft complaints—over 685,000—received by the Federal Trade Commission in 2005. *Id.* at 2.

[2] *Id.* at 4.

[3] 542 U.S. 296 (2004).

States v. Booker[4] on the charging and prosecution decisions in Internet fraud cases. Part V discusses the value of prosecuting the Internet fraud case as a misdemeanor as well as considering other viable charges. Part VI discusses working with federal authorities to get the Internet fraudsters prosecuted. Part VII explores some non-prosecution methods to help potential and actual Internet fraud victims. Finally, Part VIII reviews some lessons from the field—ideas generated from successfully prosecuted Internet fraud cases. The overarching goal is to empower the reader with methods for ensuring that costly Internet fraud cases are pursued in some fashion that results in a safer Internet experience for all.

II. BUILDING THE CASE

A. A Crime Tied to Victims

Most fraud cases perpetrated through the use of the Internet or over a computer are dependent upon proof of a specific amount of loss—the higher the amount of loss, the greater the penalty. For example, Michigan law criminalizes intentionally accessing a computer system to execute a scheme to defraud.[5] The statutory penalty for this crime varies from a ninety-three-day misdemeanor to a ten-year felony depending upon the amount of loss involved.[6] In order to convict a person of a felony, the prosecutor needs to prove a minimum of $1000.00 loss. In calculating the statutory amount of loss, the prosecutor is authorized to aggregate the loss to "a victim or group of victims" during any "12-month period" of time.[7]

---

[4] 543 U.S. 220 (2005).

[5] MICH. COMP. LAWS § 752.794 (2000). Throughout this article, Michigan law is provided as an example. It is not the intention of the author to present Michigan law as a model for the country—Michigan law is far from perfect in simplifying the prosecution of computer crimes. The reader is urged to consider the applicability of similar state laws within his or her state. In the absence of similar state laws, the reader is urged to present new legislation to the appropriate state authorities.

[6] *Id.* § 752.797 (2000). Under the statute, a loss less than $200.00 is punishable as a ninety-three-day misdemeanor; a loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor; a loss between $1000.00 and less than $20,000.00 is punishable as a five-year felony; and a loss in the amount of $20,000.00 or more is punishable as a ten-year felony. *Id.*

In the hypothetical discussed in Section I.A., the prosecutor needs to find ten victims in order to prove an aggregate loss of over $1000.00. How can law enforcement find victims that are willing to travel to court to testify in order to prove the minimum amount of loss? Have victims been identified that the prosecutor can "afford" to use—that do not have too far to travel and hence are not too costly to the office? How does law enforcement determine the extent of the fraud?

B. Important Partnerships

1. The Federal Trade Commission

The Federal Trade Commission (FTC) has developed a consumer complaint database entitled Consumer Sentinel. "Consumer Sentinel collects information about consumer fraud and identity theft from the FTC and over 150 other organizations and makes it available to law enforcement partners across the nation and throughout the world for use in their investigations."[8] Contributors to this database include various governmental and corporate entities including, but not limited to, the Federal Bureau of Investigation and the Internet Crime Complaint Center.[9] Law enforcement can access this database—and specifically receive fraud information pertinent to one's jurisdiction—simply by becoming a member of Consumer Sentinel.[10] Through use of this resource, law enforcement may be able to gain information about more victims defrauded by their suspect. In the process, they may also be able to identify victims within their state (or nearby) that won't be too costly to use as witnesses in the Internet fraud case.

---

[7] *Id.* § 752.792(2). The Michigan Legislature amended this statute in 2000 to allow for aggregation of loss incurred by a "group of victims." *Id.* Prior to the amendment, the statute only allowed aggregation of loss incurred by a single victim—a statutory structure not conducive to Internet fraud cases involving multiple one-time victims who have only lost a small amount. *Id.*

[8] *See* FEDERAL TRADE COMMISSION, *supra* note 2, at 2.

[9] *Id.* "The Internet Crime Complaint Center (IC3) is a partnership between the [FBI] and the National White Collar Crime Center (NW3C)." Internet Crime Complaint Center, Welcome to IC3, http://www.ic3.gov (last visited Feb. 3, 2007). Information about NWC3 is available at http://www.nw3c.org; information about the IC3 is available at http://www.ic3.gov. IC3's mission, in relevant part, reads as follows: "For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes." *Id.*

2. Private Entities Such as eBay

Prosecutors of credit card fraud often suggest that credit card companies care little about stopping the fraud by assisting in the prosecution—the bottom line concern seems to be how the credit card entity will recoup from the financial loss. While this belief is likely grounded in actual experience, not all private entities are unwilling to work with law enforcement. One entity worth noting—especially because of the large amount of Internet auction fraud[11] in the last several years—is eBay.

A review of eBay's privacy policy demonstrates that this company is responsive to the needs of law enforcement. Under "Our Disclosure of Your Information," the eBay privacy policy explicitly states, in relevant part:

> We may also share your personal information with . . . law enforcement or other governmental officials, in response to a verified request relating to a criminal investigation or alleged illegal activity; (In such events we will disclose name, city, state, telephone number, email address, User ID history, fraud complaints, and bidding and listing history.).[12]

It is apparent from a reading of this section that a "verified request" does not mean a subpoena or court order because this section ends with the following statement:

> Without limiting the above, in an effort to respect your priva-

---

[10] *See* FEDERAL TRADE COMMISSION, *supra* note 2, at app. A1-A3.

[11] *Id.* at 3 ("Internet Auctions was the leading complaint category [for January-December 2005] with 12% of the overall [fraud] complaints.").

[12] eBay Privacy Policy, http://pages.ebay.com/help/policies/privacy-policy.html (last visited Feb. 3, 2007).

> cy and our ability to keep the community free from bad actors, we will not otherwise disclose your personal information to law enforcement, other government officials, or other third parties without a subpoena, court order or substantially similar legal procedure, except when we believe in good faith that the disclosure of information is necessary to prevent imminent physical harm or financial loss or to report suspected illegal activity.[13]

According to eBay personnel, this "verified request" can be satisfied with a facsimile request with office letterhead.[14]

Further exploration of the eBay website reveals a section entitled "Security and Resolution Center" where eBay provides "Police Blotter" updates of cases in which fraudsters have been caught and prosecuted.[15] This webpage further provides law enforcement with links to search for publicly available data on eBay such as "seller ID" and "active listings," information on classes for law enforcement on how eBay works, and contact numbers to communicate with eBay's "Fraud Investigation Team."[16] Even a cursory review of this information substantiates that eBay is dedicated to working with law enforcement and wants the fraudsters to be pursued.

Finally, criminal investigations into Internet fraud will be enhanced by working closely with eBay's Fraud Investigation Team (FIT). According to eBay personnel, their business keeps its records for two years.[17] FIT has access to many investigative tools and contact information and can provide helpful tips on how to get the most out of a request for these records—such as ensuring that the request covers archived documents retained by eBay, data concerning other incidents involving the same suspect, other screen names used by the suspect, and information regarding others victimized by the suspect.[18] Significantly, eBay does *not* charge for searching for and providing the information officially requested by law enforcement[19]—not something that many private entities are willing to do.

---

[13] *Id.*

[14] Telephone Interview with Jack Christin, Jr., eBay Trust & Safety Counsel (Jan. 6, 2006).

[15] eBay Security and Resolution Center, http://pages.ebay.com/securitycenter/law_case_study.html (last visited Feb. 3, 2007).

[16] *Id.*; eBay Law Enforcement Center, http://pages.ebay.com/securitycenter/law_enforcement.html (last visited Feb. 3, 2007). Another interesting link on the law enforcement page introduces l.e.a.d.s.online, "the nation's largest online investigative system in use by law enforcement for the investigation of crimes involving property." eBay Law Enforcement Center, *supra.* eBay states that it "makes listings from internet drop-off stores that list items on eBay available to law enforcement in the l.e.a.d.s.online searchable database." *Id.; see also* LeadsOnline Web-based Investigation System, http://www.leadsonline.com (last visited Feb. 3, 2007).

[17] Telephone Interview with Jack Christin, Jr., eBay Trust & Safety Counsel

III. COSTS ASSOCIATED WITH PRELIMINARY EXAMINATIONS

A. *Know Your Court*

In the hypothetical described in Section I.A., in order to charge the Internet fraud as a felony, the prosecutor needs to gain the cooperation of at least ten victims (most of whom reside out of state). The anticipated cost for travel, food and accommodations for the preliminary examination through trial is over $10,000.00. The charging decision is often based on what the office can afford. Are there ways to keep these costs down at a preliminary examination?[20]

In general, prosecutors working for a state Attorney General Office practice law in county circuit courts all over the state. While the prosecutor might be well-versed in the law, is he aware of the typical court procedure in a given county? Does he know what a particular judge expects or will allow in his courtroom? It is essential to have contacts to call on—a phone call can resolve a lot of uncertainty on how to best proceed.

One potential cost-saving example—where it will be vital

(Jan. 6, 2006). Moreover, eBay maintains possession of Pay Pal records dating back to 1998. *Id.*

[18] *Id.*

[19] *Id.*

[20] Of course, costs associated with witness travel will still be present if the case goes to trial. The "accused" has the right "to be confronted with the witnesses against him." U.S. CONST. amend. VI. Nevertheless, if the costs associated with a preliminary examination are reduced, the prosecutor might be able to afford to bring in the necessary witnesses for trial. In addition, once past the preliminary exam the defendant might plead guilty—thus, avoiding the costs altogether.

to know in advance how the court might react—involves commencing a preliminary exam[21] within the statutory time frame[22] but then asking the court for an adjournment to incur the costs associated with witness travel only when it is clear that the preliminary examination will go forward. While most states require a preliminary examination to commence within a certain time period, many do not require that the exam be *completed* within that period.[23] Many state statutes authorize the delay or adjournment of a preliminary examination for "good cause."[24] Does state case law exist that holds "good cause" is present when the prosecutor is trying to avoid significant unnecessary costs? Even if there is case law on point, how will the particular judge react to this request? It might be time to pick up the phone and call your contact.[25]

B. Establishing Probable Cause with Hearsay Testimony

Of course, the costs associated with witness testimony are non-existent when a witness does not have to appear to testify. At a preliminary examination in federal court, the "finding of probable cause may be based upon hearsay evidence in whole or in part."[26] This is likely due to the fact that a federal grand jury indictment may also properly be based upon hearsay evidence.[27] Some states also permit the prosecutor to use hearsay evidence at a preliminary examination.[28]

---

[21] This example is predicated upon the assumption that hearsay testimony is not admissible at the preliminary examination to establish the victim fraud.

[22] Many states require the preliminary examination to commence within fourteen days of a defendant's initial appearance on a complaint. *See, e.g.*, MICH. COMP. LAWS § 766.4 (2000).

[23] *See, e.g.*, People v. Lewis, 408 N.W.2d 94 (1987) (where preliminary examination is started within fourteen days, there is no requirement to complete the exam within fourteen days).

[24] *See, e.g.*, MICH. COMP. LAWS § 766.7 (2000).

[25] Another alternative is a mandatory status conference—scheduled well before any preliminary examination date. Such an event might be useful in helping to determine whether or not the defendant is likely to waive his right to a preliminary exam.

[26] FED. R. CRIM. P. 5.1 advisory committee's note.

[27] Costello v. United States, 350 U.S. 359 (1956).

[28] *See, e.g.*, UTAH CONST. art. 1, § 12 ("Nothing in this constitution shall pre-

However, even if a state generally requires non-hearsay evidence, statutes or rules may exist that authorize, in part, the use of hearsay testimony.[29] For example, Michigan Rule of Evidence 1101(b)(8) provides that at a preliminary examination "hearsay is admissible to prove, with regard to property, the ownership, authority to use, value, possession and entry."[30] What witnesses in the hypothetical at Section I.A. might be included within this rule? Arguably, all of the victims should be included as the "authority to use" or "ownership" of their "property" (money or credit card information) is at issue. Additionally, representatives from eGads should be included as the "authority to use" the business "property" (the website) is at issue. Used properly,[31] such a rule can greatly simplify and reduce the cost of a preliminary examination—it might eliminate the need for all witnesses except the investigating officer. Once again, it would be a good idea to find out ahead of time if the particular court one will appear before is receptive to such a practice.

---

clude the use of reliable hearsay evidence as defined by statute or rule in whole or in part at any preliminary examination to determine probable cause or at any pretrial proceeding with respect to release of the defendant if appropriate discovery is allowed as defined by statute or rule.").

[29] *See, e.g.*, KAN. CRIM. PROC. CODE ANN. § 22-2902(3) (West 2006) ("When the victim of the felony is a child less than 13 years of age, the finding of probable cause as provided in this subsection may be based upon hearsay evidence in whole or in part presented at the preliminary examination by means of statements made by a child less than 13 years of age on a videotape recording or by other means."); N.M. METRO CT. R. CRIM. P. 7-608 (West 2006) (hearsay evidence of controlled substance test and autopsy results admissible at preliminary hearings).

[30] MICH. R. EVID. 1101(b)(8). This provision was added effective May 14, 2001. *Id.* at note (Note to 2001 Amendment). The Note to the 2001 Amendment provides: "In property crime cases, it allows the use of hearsay to prove certain elements of property crimes at the preliminary examination." *Id.*

[31] To increase the likelihood that a court will allow for such an approach, the case investigator should be directed to get some kind of written certification from the witnesses. "Certified records of regularly conducted activity" are self-authenticating under FEDERAL RULE OF EVIDENCE 902(11) and similar state rules. *See, e.g.*, MICH. R. EVID. 902(11). In the alternative, a written and signed statement from the investigating officer revealing the victim's comments regarding the "property" at issue will be of value in persuading the court.

C. Testimony through Telephonic, Voice or Video Conferencing

Even if a rule comparable to Michigan Rule of Evidence 1101(b)(8) does not exist in one's state, low cost alternatives for obtaining witness testimony may be available. Under Michigan law, on a "motion of either party" and "upon a showing of good cause," the testimony of "any witness" may be "conducted by means of telephonic, voice, or video conferencing."[32] Does the courthouse have the technical capacity to conduct this kind of examination? If so, would the court consider the extraordinarily high expense of travel and accommodations as "good cause" for allowing the testimony by telephone or other means? As courtrooms across the country become better equipped to handle advances in technology,[33] the judges in those courtrooms may be more willing to use high tech means for bringing in the testimony of victim witnesses at preliminary hearings.

D. Who Will Pay for the Travel?

It seems to be a common concern: United States citizens want less taxes and more money in their pockets. But how far can the "cuts" go before law enforcement can only "afford" to investigate and prosecute the most violent crimes? In light of this dilemma, might Internet fraud victims be amenable to the request that they "pay their way" to the courthouse? If the choice is between a declination and a prosecution, some victims may be willing to absorb the cost.[34] Moreover, if the victim understands that the only way to get restitution is by being a witness—and the potential amount for restitution exceeds the cost of travel—the incentive for the witness to finance his or her own travel may rise significantly.[35]

---

[32] MICH. COMP. LAWS § 766.711a (2000).

[33] According to DOAR Litigation Consulting, their company has "installed over 500 high-tech courtrooms nationwide." *See* DOAR Litigation Consulting, Trial Technology, http://www.doar.com/litigation-consulting-services/trial-presentation/trial-presentation-technology.asp (last visited Feb. 3, 2007).

[34] Businesses that need to provide a witness to testify might also be willing to waive the costs of travel. While the private entity might not be willing to offer this publicly (on the website or otherwise), the entity might be willing to help out on a case by case basis. Of course, this suggestion is equally applicable to trial witnesses as it is to preliminary examination witnesses.

Additionally, a state may have a witness expense fund that could be used to finance witness travel.[36] For example, the State of Maryland collects court costs in a variety of situations[37] and then authorizes the use of those funds "to relocate victims and witnesses to protect them or to facilitate their participation in court proceedings."[38] Even if witness travel is not specifically included, there may be a statute that authorizes the court to order a defendant to pay costs associated with the investigation and prosecution of the defendant.[39]

E. Is a Preliminary Examination Really Needed?

The Michigan Legislature is presently considering legislation that would eliminate the general right to a preliminary examination for felony crimes.[40] Upon the motion of either party and for "good cause," a court could order a preliminary examination if the maximum sentence for the underlying felony charge was imprisonment for ten years or more.[41] According to Michigan Attorney General Mike Cox, "[s]tudies show that 75% of preliminary exams are waived by defendants, but only after police officers, victims, and other witnesses have spent hours in court."[42] Moreover, Cox notes, the legislature can eliminate preliminary exams because they are a "statutory right, not a constitutional right."[43] Not surprisingly, the legislation is vigorously opposed by civil liberties groups.[44] While passage of the legislation is far from clear, it certainly presents an alternative that would simplify and reduce the cost of Internet fraud prosecutions.[45]

---

[35] This idea was discussed in detail by Todd Lawson, Assistant Attorney General, Office of the Attorney General of Arizona, in a panel discussion on "The Decision to Prosecute," during an April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General.

[36] This idea was provided by Carolyn Henneman, Assistant Attorney General, Office of the Attorney General of Maryland, during the presentation of this paper at an April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General.

[37] *See* MD. CODE ANN., CRIM. PROC. § 7-301 (West 2006).

[38] *See* MD. CODE ANN., CRIM. PROC. § 11-904 (West 2006).

[39] *See, e.g.,* MICH. COMP. LAWS § 769.1f (2000).

[40] *See* H.B. 4796, H.B. 4797, H.B. 4799, H.B. 4800, 2005 Leg., 2005-2006 session (Mich. 2006). For a summary of the legislation, visit the Michigan Legislature website. Senate Fiscal Agency, Committee Summary (2006), http://www.legislature.mi.gov/documents/2005-2006/billanalysis/Senate/htm/2005-SFA-4796-S.htm.

[41] *Id.*

IV. SENTENCING GUIDELINES AND THE *BOOKER* PROBLEM

A. Booker *Background*

The Federal Sentencing Guidelines (hereinafter "Guidelines") were implemented in 1987 as a response to Congress' perception that defendants around the nation were receiving widely disparate sentences depending on the judge, location, offense, and other factors.[46] The Guidelines provided a mandatory formalistic approach which limited the judge's role or discretion while expanding the traditional role of the prosecutor in determining the sentence imposed. Many states also have their own form of sentencing guidelines—some of the guidelines are mandatory and some are discretionary.[47]

---

[42] Press Release, Office of the Attorney General, Mike Cox, Attorney General, More Cops on the Street Proposal Unveiled (May 11, 2005), *available at* http://www.michigan.gov/ag/0,1607,7-164-34739_34811-117788—,00.html.

[43] *Id.*

[44] *See, e.g.,* Press Release, American Civil Liberties Union of Michigan, ACLU Opposes Cox's Support for Elimination of Preliminary Examinations (May 10, 2005), *available at* http://www.aclumich.org/modules.php?name=News&file=print&sid=419.

[45] According to audience participants during the presentation of this paper at the April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, several states, including Colorado, Maryland and Florida, have adopted laws with similar provisions.

[46] United States Sentencing Commission, http://www.ussc.gov (last visited Feb. 3, 2007). For more information, visit the United States Sentencing Commission's website. *Id.*

[47] *See* National Center for State Courts, Knowledge and Information Services: Sentencing FAQs, http://www.ncsconline.org/WC/FAQs/SentenFAQ.htm (last visited Feb. 3, 2007); *see also* U.S. Dept. of Justice, State Court Organization 1998,

Over the last six years, however, through various decisions of the United States Supreme Court,[48] including *United States v. Booker*,[49] and *Blakely v. Washington*,[50] the Court has deemed mandatory sentencing guidelines unconstitutional under the Sixth Amendment, thus rendering them advisory rather than mandatory. In *Booker*, the Court held that "[a]ny fact (other than a prior conviction) which is necessary to support a sentence exceeding the maximum authorized by the facts established by a plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt."[51] In other words, the Sixth Amendment requires juries, not judges, to find facts relevant to sentencing.[52]

While subject to interpretation in the courts, *Booker* and *Blakely* appear to have an impact only in those states with mandatory sentencing guidelines—they do not affect sentencing in those jurisdictions where sentencing guidelines are wholly discretionary.[53] As one commentator stated, "The very breadth of their discretion seems to somehow insulate them from jury

---

http://www.ojp.usdoj.gov/bjs/pub/pdf/sco9807.pdf (last visited Feb. 3, 2007).

[48] United States v. Booker, 543 U.S. 220 (2005) (reviewed federal sentencing guidelines); Blakely v. Washington, 542 U.S. 296 (2004) (reviewed Washington's sentencing guidelines); Apprendi v. New Jersey, 530 U.S. 466 (2000) (examined New Jersey sentencing scheme). A full discussion of these cases is beyond the scope of this article. *See generally* Rosemary T. Cakmis, *The Role of the Federal Sentencing Guidelines in the Wake of* United States v. Booker *and* United States v. Fanfan, 56 MERCER L. REV. 1131 (2005); *see also* Douglas J. Fries, *The Federal Sentencing Guidelines Weight-Loss Plan: Just How Mandatory are the "Advisory" Guidelines After* United States v. Booker?, 55 CASE W. RES. L. REV. 1097 (2005); Jennifer M. Murray, Note, Blakely v. Washington*: The End of Sentencing Guidelines and the Re-Emergence of Judicial Discretion*, 6 LOY. J. PUB. INT. L 217 (2005).

[49] 543 U.S. 220 (2005).

[50] 542 U.S. 296 (2004).

[51] *Booker*, 543 U.S. at 244.

[52] Regarding sentences handed down prior to *Booker* and *Blakely*, the United States Supreme Court recently held that appellate courts can rely on a harmless error analysis in reviewing those sentences. Washington v. Recuenco, 126 S. Ct. 2546 (2006).

[53] See, for example, *People v. McCuller*, 715 N.W.2d 798 (Mich. 2006), and *People v. Drohan*, 715 N.W.2d 778 (Mich. 2006), where the Michigan Supreme Court held that Michigan's sentencing guidelines do not violate *Blakely* because the guidelines score the minimum range of an indeterminate sentence.

trial scrutiny."[54] States with discretionary or indeterminate sentencing guidelines seem to remain free from constitutional trouble even though judges in those states may engage in "invisible" fact finding in arriving at the appropriate sentence.

B. Booker *Relevancy to Internet Fraud Cases*

How ought a state with mandatory sentencing guidelines approach the charging decision in an Internet fraud case? If a prosecutor hopes to hold a defendant accountable at sentencing for a specific amount of fraud loss, the full amount of loss needs to be proved before a jury. Just as with other elements of a crime on which a conviction is based, calculating the amount of loss which has an effect on a defendant's conviction must be proven to a jury beyond a reasonable doubt.

United States v. Davis,[55] a mandatory guidelines case, is instructive. In *Davis*, the sentencing judge independently made factual findings of the amount of loss, which enhanced the defendant's sentence for bank fraud beyond the facts established by the jury verdict. The court found that, just as Booker's sentence was based on independent fact-finding and thus violated the Sixth Amendment, this sentence, too, violated the Sixth Amendment.[56] Therefore, the court remanded the case for resentencing.

So what does this mean for the Internet fraud prosecution? In a jurisdiction with "mandatory" sentencing guidelines, it appears that the prosecutor should include some kind of reference—in the charging document—to the victims he wants to hold the defendant accountable for at sentencing.[57] Of course, that means that the prosecutor needs to know early on in the prosecution which victims he can "afford" to include in the charging document. Once again, the high costs might present an insurmountable barrier. Are there ways to reduce the costs?

---

[54] Robert Weisberg, *Excerpts from "The Future of American Sentencing: A National Roundtable on* Blakely", 2 OHIO ST. J. CRIM. L. 619, 646 (2005) (quoting Kevin Reitz, Professor of Law, University of Colorado).

[55] 397 F.3d 340 (6th Cir. 2005).

[56] *Id.* at 350-51.

[57] Due to *Booker*, many federal courts now view the United States Sentencing Guidelines as merely advisory. This approach allows trial judges to continue with judicial fact-finding at sentencing—without violating the Sixth Amendment. *See, e.g.*, United States v. Owens, 441 F.3d 486, 490 (7th Cir. 2006) ("*Booker* clearly permits a district court to grant a sentencing enhancement based on facts not

C. *Value of Plea Agreements*

In *United States v. Murdock*,[58] the defendant contended that his sentence for causing another to possess false documents with intent to defraud must be vacated because the judge decided the amount of loss without submitting the issue to the jury for a determination of loss beyond a reasonable doubt. The Sixth Circuit Court of Appeals held, however, that there was no Sixth Amendment violation because the sentencing court's determination of the amount of loss was supported by the defendant's admission in the plea agreement and at the plea hearing regarding the amount of loss. As held in *Booker*, the court noted that sentencing facts "established by a plea of guilty or a jury verdict" do not violate the Sixth Amendment.[59]

What does *Murdock* (and cases similarly decided) mean for Internet fraud prosecutions? Plea agreements provide a means to reduce the costs of prosecuting an Internet fraud case.[60] As *Booker* does not appear to prohibit reliance on a defendant's own admissions, a prosecutor might work to generate a plea agreement involving an agreement to a specific amount of fraud loss. Defendant might agree in a plea to a certain amount of fraud loss in exchange for the prosecutor not pursu-

---

charged in the indictment, not proven to a jury beyond a reasonable doubt or not admitted by the defendant.") (citing United States v. Booker, 543 U.S. 220, 226-27 (2005)); United States v. Gonsalves, 435 F.3d 64, 72 (1st Cir. 2006); United States v. Crosby, 397 F.3d 103, 112 (2d Cir. 2005).

[58] 398 F.3d 491 (6th Cir. 2005).

[59] *Id.* at 501 (quoting *Booker*, 543 U.S. at 244); *see also* United States v. Bradley, 400 F.3d 459, 462 (6th Cir. 2005) (the Sixth Amendment and *Booker* do not apply to "agreed-upon facts"), *cert. denied*, 126 S. Ct. 145 (2005).

[60] *See* Barry Boss & Nicole L. Angarella, *Negotiating Federal Plea Agreements Post-*Booker*: Same as It Ever Was?* 21 CRIM. JUST. 22, 25 (2006) ("Although it is important to understand this new sentencing landscape and consider it in negotiating a plea deal with the government, the reality is that the new system has not brought any radical change to plea or sentencing practices.").

ing a greater amount of loss and victims.[61] The defendant might have an incentive to agree to this kind of an offer if he thinks he can avoid prosecution for a greater amount of loss.[62]

D. Booker*'s Impact on Restitution*

In *United States v. Sosebee*,[63] defendant challenged the validity of the restitution order in light of *Booker*. She argued that her sentence violated her Sixth Amendment rights because the restitution order was based on a factual determination by the district court that was neither found beyond a reasonable doubt by a jury nor admitted by the defendant. Noting that even though restitution may be considered punishment, the *Sosebee* court nevertheless held that restitution orders are not affected by the Supreme Court's recent ruling in *Booker*.[64]

According to the *Sosebee* court, restitution orders are authorized by statute[65] and in that sense are "distinct and separate from the United States Sentencing Guidelines."[66] The court noted that "[a]lthough the guidelines mandate imposition of restitution where allowable under the statutes, the restitution statutes function independently from the guidelines and do not rely on the guidelines for their validity."[67] Furthermore,

---

[61] Of course, the prosecutor is only capable of binding his or her own office. Prosecutors in other states could still pursue a case in their state assuming they have proper jurisdiction. The likelihood of this occurring, however, is quite small—especially if the defendant resides in the state in which the defendant pleaded guilty.

[62] Nevertheless, it will be difficult for a prosecutor to have the capability to work this kind of agreement if the defense bar thinks the prosecutor's office will not work the case because they can't afford it.

[63] 419 F.3d 451 (6th Cir. 2005).

[64] Several other circuits have also held that *Booker* does not apply to restitution orders under the Victim and Witness Protection Act or the Mandatory Victim Restitution Act. *See, e.g.*, United States v. Belk, 435 F.3d 817 (7th Cir. 2006); United States v. Craiglow, 432 F.3d 816 (8th Cir. 2005); United States v. Garza, 429 F.3d 165, 170 (5th Cir. 2005); United States v. Visinaiz, 428 F.3d 1300 (10th Cir. 2005); United States v. Bussell, 414 F.3d 1048 (9th Cir. 2005); United States v. May, 413 F.3d 841 (8th Cir. 2005); United States v. George, 403 F.3d 470 (7th Cir. 2005). *See also Sosebee*, 419 F.3d at 461 (citing cases).

[65] 18 U.S.C. §§ 3663, 3663A, 3664 (2000).

[66] 419 F.3d. at 462.

[67] *Id.*

"the Victim and Witness Restitution Act and the Mandatory Victim Restitution Act specifically state that the amount of restitution should be equal to the 'amount of each victim's losses *as determined by the court*.'"[68] Thus, *Booker*'s holding that the Sentencing Guidelines are now merely advisory does not appear to affect orders of restitution.[69]

The *Sosebee* lesson appears to be that a prosecutor can ask the sentencing court for a restitution amount higher than the fraud amount proved beyond a reasonable doubt before the jury.[70] In addition to helping reduce the cost of prosecution, this might provide the prosecutor with some negotiating leverage.

V. ALTERNATIVE PROSECUTION ROUTES

A. *Misdemeanor Charges*

When making the determination of how to spend precious budget dollars, some jurisdictions appear to place higher priority on felony convictions. But what's so bad about a misdemeanor conviction? In all likelihood, acceptance of a misdemeanor conviction as a valuable remedy for Internet fraud—by law enforcement and, to a lesser extent, the public—is the biggest barrier. When the choice becomes declination or a prosecution, however, a misdemeanor is a valuable alternative. Moreover, there are some fairly strong reasons to consider misdemeanor convictions as the best choice.

In the hypothetical described in Section I.A., the suspect company had a presence in the State of Chaos and at least one victim within the State of Chaos—a victim who had lost $250.00. Under a typical fraud statute, this crime could be prosecuted as a one-year misdemeanor.[71] Such a conviction, at a minimum, serves to satisfy the local interests in a prosecution. Moreover, the cost of the prosecution is manageable—whether hearsay is permitted at a preliminary examination or not. Finally, the likelihood of collecting restitution—and actually providing the victim with money to recoup his losses—is much higher with such a conviction. One victim, a local defendant, and a small amount of loss—these facts do not present an insurmountable barrier to collection of the loss. In the long run, few fraud victims are happier than those that actually get their money back.

---

[68] *Id* (emphasis in original) (quoting 18 U.S.C. § 3664(f)(1)(A) (2000)).

[69] *Id.*

[70] While *Sosebee* involved federal restitution laws, a similar analysis arguably applies to state restitution laws.

[71] *See, e.g.*, MICH. COMP. LAWS § 752.797(1)(b)(i) (2000) (loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor).

B. Identity Theft

For various reasons, a prosecutor might consider charging an Internet fraud case as an identity theft case. Numerous states have passed laws addressing the problems of identity theft.[72] Oftentimes, a financial fraud case can easily be recharacterized as an identity theft case. For example, considering the hypothetical in Section I.A., further investigation may reveal that the post office box located in Cooley City, Chaos, was set up with the unauthorized personal identifying information of another person living in the State of Chaos. Some excellent reasons exist for considering this case as an identity theft matter.

Unlike Internet fraud statutes, identity theft statutes are generally not based upon proof of an amount of loss.[73] The paramount concern in identity theft cases is not the money lost—it is the unauthorized usage of another's personal identifying information.[74] Therefore, an amount of loss is neither

---

[72] *See* Federal Trade Commission, Your National Resource About ID Theft, http://www.consumer.gov/idtheft/id_laws_state_criminal.htm (providing a listing of numerous state and federal laws and agencies dealing with identity theft). Some states, like Michigan, are passing comprehensive identity theft statutes that provide both civil and criminal remedies as well alternatives for the identity theft victim to help himself. *See, e.g.*, MICH. COMP. LAWS §§ 445.61-77 (West 2006).

[73] *See, e.g.*, MICH. COMP. LAWS §§ 445.65-69 (West 2006).

[74] The Michigan law provides one example of a definition of "[p]ersonal identifying information":

> [A] name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial

needed nor relevant. Quite obviously, this means fewer witnesses are needed (and, hence, a reduction in cost of prosecution in comparison to the Internet fraud case).

Moreover, in many states, using an identity theft statute provides a prosecution for a felony rather than a misdemeanor.[75] Oftentimes, the statutory maximum penalty for identity theft exceeds that for Internet fraud—especially when comparing the available penalty for the Internet fraud prosecution that involves only the low cost local victims (likely a misdemeanor).[76] The high available penalty for identity theft would certainly seem to satisfy the law enforcement entities concerned with ensuring that their precious dollars are allocated in a high impact fashion.

C. Enhancing the Penalty and Plea Negotiations With Computer Crime Statutes

In the hypothetical discussed in Section I.A., the defendant did not merely commit identity theft. By using a computer system to offer up bogus products and provide a payment method involving a post office box obtained in another's name, he also committed a computer crime.

State legislatures often consider usage of a computer to

> accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

Id. § 445.63(k).

[75] *See, e.g.*, *id.* § 445.69(1).

[76] *Id.* ("[A] person who violates section 5 or 7 is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than $25,000.00, or both."); *cf. id.* § 752.797 (loss less than $200.00 is punishable as a ninety-three-day misdemeanor; loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor; loss between $1000.00 and less than $20,000.00 is punishable as a five-year felony; and loss in the amount of $20,000.00 or more is punishable as a ten-year felony).

commit a crime—even a traditional crime—a more serious criminal act.[77] The mere fact that a computer or computer system was used to facilitate the crime makes the act more severe. For example, Michigan law provides: "A person shall not use a computer program, computer, computer system, or computer network to commit, attempt to commit, conspire to commit, or solicit another person to commit a crime."[78] This charge is *in addition to* any other crime committed during the time in question including the underlying offense the computer was used to commit.[79]

Even more significant, however, is the potential for an enhanced penalty. Oftentimes the penalty is tied to the crime that the computer was used to commit.[80] By way of illustration, assume that the crime of identity theft is a five-year felony. Under Michigan law, using a computer to commit this five-year felony would be punishable as a separate seven-year felony.[81] In addition, the law might provide for a consecutive sentence[82]—which certainly enhances the potential for effective plea negotiations. Quite obviously, effective and low-cost prosecution alternatives exist—but the prosecutor needs to think beyond merely considering the case as a monetary scheme to defraud.

---

[77] *See, e.g., id.* § 752.796(1).

[78] *Id.*

[79] *Id.* §§ 752.796(2)-(3).

[80] *Id.* § 752.797(3).

[81] *Id.* ("If the underlying crime is a felony with a maximum term of 4 years or more but less than 10 years, the person is guilty of a felony punishable by imprisonment for not more than 7 years or a fine of not more than $5,000.00, or both.").

[82] *Id.* § 752.797(4) ("The court may order that a term of imprisonment imposed under subsection (3) be served consecutively to any term of imprisonment imposed for conviction of the underlying offense."). The Michigan legislature permits a consecutive sentence within the discretion of the sentencing court. Even greater potential would exist if this law required mandatory consecutive sentences.

VI. WORKING WITH FEDERAL AUTHORITIES

A. *Connection with Federal Authorities*

Ideally, the Internet fraud case that is investigated by local or state authorities should be prosecuted in the state courts. Frequently, however, law enforcement concludes that prosecuting the Internet fraud case in state court is cost-prohibitive. Given the "deeper pockets" of the federal government, there are some strong reasons to consider working with the federal authorities to get the case prosecuted in federal court.[83]

Initially, it helps to realize that the United States Attorneys Offices do *not* want to steal state cases![84] This seemingly widespread belief likely stems from the fact that once a case becomes a federal case, it must comply with the federal criminal justice system. This includes a defendant's right to be prosecuted through a grand jury indictment.[85] Federal grand jury proceedings are governed by a general rule of secrecy—a knowing violation of this may be punished as a contempt of court.[86] This might help explain the lack of a free flow of information between the state and federal authorities once the case becomes a federal case. The lack of communication that follows may induce state and local officers to believe that the federal government does not want to work with the states—a belief that is generally untrue.

The hypothetical discussed in Section I.A. involved some forty-five witnesses throughout the country with a total loss amount of approximately $20,000.00. Given the fact that the Chaos defendant victimized people from all over the country—thus impacting on interstate commerce—it appears on its face to be worthy of federal consideration. How does a state prosecutor go about getting a case prosecuted in federal court?

---

[83] Of course, *United States v. Booker*, 543 U.S. 220 (2005), and its implications on the federal charging decision as well as the federal sentencing, needs to be considered. *See supra* notes 47-70 and accompanying text.

[84] This statement is based upon the personal experience of the author while working in the United States Attorney's Office for the Eastern District of Michigan from 1989-1999.

[85] U.S. CONST. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . .").

[86] FED. R. CRIM. P. 6(e)(2), (7).

At the outset, it helps if the local and state investigators have contacts within the federal system. Many federal law enforcement agencies investigate fraud cases.[87] These contacts can, at a minimum, provide the connection to get a case considered for federal prosecution.

Preferably, however, the local and state investigators won't merely have federal contacts. Internet fraud task forces—comprised of both state and federal authorities—provide the most efficient means for choosing the correct forum for prosecution. Some task forces might also work closely with private industry.[88] Working side by side, maybe even assisting in each other's search warrants, law enforcement officers will know from the beginning whether a case should be prosecuted in state or federal court.

B. *Internal Prosecution Guidelines*

Of course, federal law exists that criminalizes Internet fraud.[89] It is important to know, however, that United States

---

[87] Based upon the personal experience of the author, the following federal agencies, amongst others, investigate fraud matters on varying levels: The Federal Bureau of Investigation, the United States Secret Service, the United States Postal Inspectors, the Internal Revenue Service-Criminal Investigation Division, United States Customs, United States Bureau of Alcohol, Tobacco and Firearms, United States Food and Drug Administrations, and the United States Department of Education.

[88] *See, e.g.*, Electronic Crimes Task Force, http://www.ectaskforce.org (last visited Feb. 3, 2007). The Electronic Crimes Task Force lists thirteen regional task force locations. Electronic Crimes Task Force, Regional Locations, http://www.ectaskforce.org/Regional_Locations.htm (last visited Feb. 3, 2007). Local offices of the United States Secret Service have information on more task force locations. *See* Infragard, Guarding the Nation's Infrastructure, http://www.infragard.net (last visited Feb. 3, 2007) (works closely with the Federal Bureau of Investigation as well as other law enforcement entities); International High Technology Crime Investigation Association, http://www.htcia.org (last visited Feb. 3, 2007).

[89] *See, e.g.*, 18 U.S.C. § 1028 (2000) ("Fraud and related activity in connection with identification documents and information"); *id.* § 1029 ("Fraud and related activity in connection with access devices"); *id.* § 1030 ("Fraud and related activity in connection with computers"); *id.* § 1341 ("Frauds and swindles"); *id.* § 1343

Attorney Offices often have internal "prosecution guidelines" before a case will be accepted for federal prosecution.[90] Using the hypothetical discussed in Section I.A., assume that the State of Chaos has two federal districts—the Eastern District of Chaos (located in a large urban area) and the Western District of Chaos (located in a smaller urban area). The Eastern District—given the larger number of fraud cases in that district—might require the fraud loss to exceed $40,000.00 before the case can be presented to a grand jury. The Western District—given that it is located in an area with less fraud—might merely require the fraud loss to exceed $10,000.00.[91] Equipped with knowledge of the prosecution guidelines, law enforcement will know from the outset if a federal prosecution can even be considered.[92]

C. *Special Assistant United States Attorneys*

Even if an appropriate federal statute exists and the Internet fraud case meets the threshold required for the prosecution guidelines of the relevant United States Attorney Office, the United States Attorney's Office might not have a federal prosecutor available to prosecute the case. In the alternative, even if a federal prosecutor is available, the state prosecutor—due to his ongoing involvement in the case—might be best situated to prosecute the matter.[93] Under those circumstances,

---

("Fraud by wire, radio, or television"); *id.* § 1344 ("Bank fraud").

[90] This information is not publicly available. One needs to contact the specific United States Attorney Office to determine if such a prosecution guideline exists in that office.

[91] Amount of loss is not the only factor that might be considered. United States Attorney Offices also consider, inter alia, factors such as the number of victims, the prevalence of the fraud, and the complexity of the crime. One needs to contact the specific United States Attorney Office to determine the specific requirements of the prosecution guidelines for that office.

[92] Of course, the full amount of loss may not be known until well into the investigation—another reason why working with a task force is a good idea. In such a scenario, a case that started out as a state prosecution might develop into a much larger fraud. If state and federal officers are jointly working the case in the context of a task force, presenting the matter to the United States Attorney Office when the larger fraud is discovered will be routine.

[93] Of course, if the only alternative is to have an existing federal prosecutor

a state prosecutor then should seek authorization to prosecute the case in federal court as a Special Assistant United States Attorney (hereinafter SAUSA).[94] Federal law[95] authorizes the United States Attorney General to "appoint Special Assistants to assist the United States Attorney when the public interest so requires."[96] Arguably, "public interest" requires such a desig-

---

pursue the case, this choice is certainly better than no prosecution at all.

[94] *See* THE UNITED STATES DEPARTMENT OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL, § 3-2.300 (August 2006), *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title3/2musa.htm#3-2.300.

[95] *See* 28 U.S.C. § 543 (2000).

[96] THE UNITED STATES DEPARTMENT OF JUSTICE, *supra* note 94. In its entirety, section 3-2.300 provides:

> Section 543 of Title 28 authorizes the Attorney General to appoint Special Assistants to assist the United States Attorney when the public interest so requires, and to fix their salaries. These Assistants are designated as Special Assistants to the United States Attorney and are appointed for the purpose of assisting in the preparation and presentation of special cases. Their salaries, if any, are a matter of agreement between the Department and the individual, and are fixed at an annual, monthly, per diem, or when-actually-employed rate. Under the appropriate circumstances, a private attorney may receive a Special Assistant appointment pursuant to 28 U.S.C. Sec. 543, with or without compensation, to assist the United States Attorney with specific matters. Such appointments raise ethics and conflict of interest issues that must be addressed. To appoint private attorneys as Special Assistant United States Attorneys pursuant to 28 USC Section 543, compensated or not, approval is required by EOUSA.
>
> Attorneys employed in other departments or agencies of the federal government may be appointed as Special Assistants to United States Attorneys, without compensation other than that paid by their own agency, to assist in the trial or presentation or cases when their services and assistance are needed. Such appointments, and appointments of Assistant United States Attorneys from one United States Attorney's office to another, may be made by the United States Attorney requiring their services.
>
> In instances where an entire United States Attorney's Office recuses itself, the Attorney General may, pursuant to 28 U.S.C. Sec. 515, appoint any officer of the Department of Justice, or any attorney specially appointed under law, to conduct any kind of legal proceeding which United States Attorneys are authorized by law to conduct, whether or not such appointee is a resident of the district in which the proceeding is brought. Said appointee specially retained under authority of the Department of Justice is appointed as a Special Assistant or a Special Attorney to the Attorney General and reports directly to the Attorney

nation when a viable federal crime exists that will otherwise be declined.

Determination of whether to grant SAUSA status is generally a wholly discretionary matter decided by the United States Attorney in the specific federal district. In general, the United States Attorney's Office has to be convinced that it helps in some prosecution goal or program area or the prosecution of a specific case.[97] Of course, it would help in gaining SAUSA status to request no salary in excess of what one is making as a state prosecutor.[98] Ideally, a state prosecutor working with a state/federal task force will have obtained the SAUSA designation in advance to maximize the capacity of the prosecutor to take the case to the most appropriate forum whenever the need arises.

D. *Benefits of Prosecuting Internet Fraud as a Federal Case*

Some significant advantages exist in gaining SAUSA status and taking an Internet fraud case to federal court. From reduced costs to simplification of the prosecution, the federal courts offer a prosecution alternative worthy of consideration.

In investigating the matter, Federal Rule of Criminal Procedure 41 provides broad authority for the issuance of search warrants.[99] If the search warrant involves Internet service providers, federal law allows federal courts to issue nationwide search warrants for unopened e-mail.[100] The only restriction on the nationwide scope of the e-mail warrant is that the issuing court must have jurisdiction over the offense under investigation.[101] This obviously holds the potential to simplify the re-

---

> General or delegee. Such appointments are executed by the Executive Office for United States Attorneys.

Id.

[97] Other than the UNITED STATES ATTORNEYS' MANUAL, data on the process for how SAUSA status is determined does not appear to be publicly available. The textual comments are the opinion of the author based upon actual experience.

[98] *Id.*

[99] FED. R. CRIM. P. 41(b).

[100] 18 U.S.C. § 2703(a) (2000).

[101] *Id.* §2703(d). Congress authorized this section as part of the PATRIOT Act

trieval of relevant evidence in an Internet fraud case.

In prosecuting the case, the federal prosecutor only needs one witness at a preliminary examination. Unlike many states, hearsay evidence is admissible at a federal preliminary examination.[102] Notably, one's entire case can be presented through the case agent assigned to the matter[103]—no victim needs to attend at all.

Due to the grand jury system, many prosecutors choose to indict a defendant before any preliminary examination occurs.[104] Like a preliminary examination, hearsay evidence is admissible in grand jury proceedings.[105] Many prosecutors choose to seek indictments from federal grand juries through the testimony of one witness—the case agent.[106] Like a federal preliminary examination, no victim needs to be present—which obviously reduces some of the initial costs associated with an Internet fraud prosecution.

In the typical Internet fraud case, witnesses live all over the United States and often out of the country.[107] Assuming the case must go to trial, the long reach of the federal government makes connecting with these witnesses easier. Trial subpoenas may be served by "a marshal, a deputy marshal, or any

---

and, as originally written, was set to "sunset" on December 31, 2005, unless renewed by Congress. President Bush recently signed legislation making this provision permanent. Alexei Alexis, *Bush Signs Bill Renewing PATRIOT Act With New Provisions to Safeguard Data*, 78 CRIM. L. REP. (BNA) 669, Mar. 15, 2006.

[102] At a preliminary examination in federal court, the "finding of probable cause may be based upon hearsay evidence in whole or in part." FED. R. CRIM. P. 5.1.

[103] Based upon the personal experience of the author, most federal preliminary exams involve no more than a few witnesses.

[104] If a federal prosecutor does this, he does not need to proceed with the preliminary examination as the determination of "probable cause" as been accomplished by the grand jury.

[105] Costello v. United States, 350 U.S. 359 (1956).

[106] This statement is based upon the personal experience of the author.

[107] Subpoenas directed to witnesses in a foreign country are discussed at 28 U.S.C. § 1783 (2000). In such a situation, the prosecutor ought to consider seeking assistance from the United States Department of Justice, Office of International Affairs. *See* United States Department of Justice, Criminal Division, Office of International Affairs, http://www.usdoj.gov/criminal/oia.html (last visited Feb. 3, 2007).

nonparty who is at least 18 years of age."[108] Moreover, the federal subpoena "requiring a witness to attend a hearing or trial may be served at any place within the United States."[109]

Finally, and maybe most importantly, any fees connected with a federal case are, of course, paid for by the federal government.[110]

VII. NON-PROSECUTION METHODS TO HELP VICTIMS

Victims of Internet fraud are nearly powerless to correct the damage caused by the fraudsters. The ideal remedy (police catching the defendant) is sometimes not realistic because the thieves are quite often in a different state, country, or even continent. Assuming the prosecutor cannot pursue the case criminally, can law enforcement help out in other ways?

The Internet is replete with sources on how to prevent fraud.[111] Information is available to help both businesses and consumers enhance the security of online transactions.[112] The biggest problem with this publicly available information is that there is simply too much information.[113] Citizens often do not know where to begin—either to prevent the fraud or to act properly once they have been defrauded.

---

[108] FED. R. CRIM. P. 17(d). Federal agents exist all over the county who can assist in serving subpoenas.

[109] FED. R. CRIM. P. 17(e)(1); *see also* 18 U.S.C. §§ 3481-3510 (2000) ("Witnesses and Evidence").

[110] *See, e.g.,* 18 U.S.C. § 3495 ("Fees and expenses of consuls, counsel, interpreters and witnesses"). Of course, United States Attorneys Offices are not exempt from having many of the financial difficulties confronted by state and county prosecutors. *See* Dan Eggen, *Lawmakers Urge Funds for U.S. Attorneys*, WashingtonPost.com, July 25, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/07/24/AR2006072400952.html.

[111] Using the term "fraud prevention," a Google search by the author on March 6, 2006, revealed 29,300,000 links to related online sources.

[112] While there are many excellent sites, one exceptional source is OnGuard Online, http://onguardonline.gov (last visited Feb, 3, 2007). On the homepage, OnGuard Online states that it "provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information." *Id.* Another great resource is Scambusters.org, http://www.scambusters.org (last visited Feb. 3, 2007). Scambusters.org provides links to articles covering just about every topic in the area of Internet fraud. *Id.* Of course, as has already been discussed, the Federal Trade Commission and the National White Collar Crime Center are also excellent resources. *See supra* notes 9-12 and accompanying text.

Law enforcement can help by disseminating good information. Prosecutors should seek authorization to speak to community groups about fraud prevention—while this may not be the traditional role of the prosecutor, it is a vital public role given the difficulties in bringing the Internet fraud cases to court. Prosecutors should consider creating a copy of an Internet fraud prevention guide or making copies available of other excellent resources.[114]

Law enforcement can help victims help themselves. Assume, for example, that the Chaos victim described in Section I.A. contacts the prosecutor's office. Believing that he has been financially defrauded, he is also worried that he may be a victim of identity theft. What help can the prosecutor provide—even if the office cannot take the case for prosecution? He can begin by introducing the victim to the resources of the Federal Trade Commission.

The Federal Trade Commission provides great advice on four immediate steps the victim should take.[115] First, the victim can prevent future damage by alerting credit reporting agencies as soon as possible and placing a fraud alert on his credit report. Second, the victim needs to close all financial accounts that he believes have been affected by the fraud. The victim needs to fill out an identity theft affidavit[116] "when disputing new unauthorized accounts."[117] Third, the victim should file a police report in the community where the fraud took place.[118] This report, along with the identity theft affidavit, will help the victim in dealing with creditors.[119] Lastly, the victim should file a complaint with the Federal Trade Commission.[120] As already discussed, [121]the Federal Trade Commission maintains a database of consumer complaints—this data might help other law enforcement authorities build a better case against the fraudster in question.[122]

---

[113] *See supra* note 112.

[114] *See* Federal Trade Commission, Consumer Publications from the Federal Trade Commission, http://www.consumer.gov/idtheft/con_pubs.htm (last visited Feb. 3, 2007).

[115] Federal Trade Commission, The FTC's Identity Theft Site, http://www.consumer.gov/idtheft/ (last visited Feb. 3, 2007).

[116] *See* Federal Trade Commission, ID Theft Affidavit, http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf (last visited Feb. 3, 2007).

[117] *See supra* note 116.

[118] In Michigan, law enforcement officials are required to provide a copy of

Law enforcement should also inform the victim about the possible availability of civil remedies. Importantly, if the proof is lacking in terms of the criminal charges ("beyond a reasonable doubt" standard), civil suits can often still prevail ("preponderance of the evidence" standard). The State Attorney General might be able to bring suit.[123] The citizen victim might also be able to bring a suit.[124] In the event a criminal prosecution is not available, law enforcement needs to know what civil remedies potentially exist. Providing information to Internet fraud victims can, at the least, give the victim a sense that the situation is not hopeless.

VIII. LESSONS FROM THE FIELD

The contents of this paper were presented at an April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of

---

that police report to victims of identity theft. *See* MICH. COMP. LAWS §§ 780.754a, 780.783b, 780.814a (2000).

[119] In providing this kind of documentation, law enforcement can provide a tremendous credibility boost for the victim in dealing with the creditors.

[120] *See supra* note 116.

[121] *See supra* notes 9-12 and accompanying text.

[122] *See also* Federal Trade Commission, *Taking Charge: Fighting Back Against Identity Theft*, February 2005, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. This document provides important details on how the victim can help himself. *Id.*

[123] In Michigan, for example, violations of Michigan's Identity Theft Protection Act are also actionable under the Consumer Protection Act as "unfair, unconscionable, or deceptive methods, acts, or practices." MICH. COMP. LAWS § 445.903(1)(jj) (2000). The Attorney General can also bring a class action suit. *Id.* § 445.910.

[124] Under Michigan law, consumers can recover actual damages or $250, whichever is greater, along with attorney fees. *Id.* § 445.911(2).

Attorneys General. Present in the audience were assistant attorneys general from all over the United States. Some of the attorneys present provided answers to questionnaires on lessons they had learned in prosecuting Internet fraud cases in their respective states. Many of the comments are interspersed throughout this article.

In particular, however, the Oklahoma Attorney General's Office provided some very helpful insights. Rather than paraphrasing the remarks from this office, the comments are provided herein in their entirety.[125] The remarks speak for themselves and are valuable in that they are the comments of a prosecutor presently working Internet fraud cases on a routine basis. As you read through the comments, pay particular attention to the suggestions regarding following the money trail to the banks and the possibility of questioning the suspect before the arrest. The remarks follow the questions presented in the questionnaire as follows:

1) Have you had success in your Internet Fraud prosecutions? If so, please explain. Please provide specific reasons why your prosecutions have been successful.

> Our office has had a 100% success rate in prosecuting Internet auction fraud cases. I believe the reason for this is threefold. First, our investigators thoroughly investigate these cases to the point that it is virtually impossible for the defense to dispute. Many times, the defendant admits guilt when questioned after being Mirandized or quickly decides to plead guilty and take a deal rather than face the uncertainty of a jury trial. How do our investigators accomplish this? After they have identified a person as a target, they send the Internet auction fraud site such as eBay a subpoena to obtain the target's records. These records contain the full registration, IP addresses, complete listing and bid history and financial information. We use this information to obtain further records including PayPal

---

[125] Special thanks to Julie A. Bays, Assistant Attorney General, Oklahoma Attorney General's Office, Consumer Protection Unit, for her thoughtful comments as provided herein.

records, credit card and banking information. We can usually follow the financial transactions directly to the target's bank account or PayPal account. In Oklahoma we also have the added benefit of a cable company that keeps IP address information for at least six months. Every time the target logs on or registers, we have the IP address for that person. It always leads right back to the target.

Secondly, our investigators usually look for potential targets that have victims residing in or near our state in order to make it practical if a witness needed to testify. If we cannot find anyone near Oklahoma, we then look for victims that are willing to travel even with the possibility of sharing some of the expense. This usually means that we find victims that have lost a large amount of money in order to make it worthwhile for them. However, we have occasionally prosecuted cases that fell under $500.00 which is our threshold for felonies. We make these decisions depending on the number of victims and the overall total loss.

Thirdly, most of the defendants we have prosecuted are first time offenders. We can offer them a deferred sentence with monthly restitution payments under our state law. The prospect of an actual conviction if tried by a jury versus no conviction at all if the defendant abides by the rules of probation provide an incentive to plead guilty and take our offer.

2) Have you faced any obstacles in your Internet Fraud prosecutions? What were those obstacles? How did you overcome them (if you did)? If you did not overcome them, please explain why.

Our biggest obstacle is the fact that many potential defendants do not meet our monetary threshold for a felony. We are seeing this in all types of internet fraud activity and I believe that state legislators need to change the statutes. For instance, phishing schemes and spam do not necessarily end up with a monetary loss and we would like to prosecute these as felonies under our state law. As I stated above, we have filed charges against persons that have

> defrauded Internet auction buyers for less than the threshold. I am not sure if my office could have afforded to fly witnesses into the state for their loss of $20.00 or so dollars each. We have overcome some of this by interviewing the defendant. For instance, in the case of *State of Oklahoma v. Maple*, we filed five misdemeanor counts only after she was Mirandized and admitted guilt to our investigators.

3) Have the *Booker* and *Blakely* decisions, and the effect those decisions had on your state sentencing guidelines, affected your ability to prosecute Internet fraud cases? If so, how? How did your office respond?

> The *Booker* and *Blakely* decisions do not affect our ability to prosecute Internet fraud cases. Our sentencing guidelines are advisory with regards to these crimes. Plus, we have not tried a case to the jury yet, but if we did, the jury would recommend the sentence within the guidelines.

4) Do you have any further comments or experiences you would like to share in relation to Internet Fraud prosecutions?

> The only comment I would like to make is that we need our state and federal laws revised regarding the monetary loss threshold in order to make it easier for prosecutors to do their jobs.

IX. CONCLUSION

There is no quick fix for Internet fraud. It is here to stay and will likely only get worse. Fraudsters need to know, however, that the sheriff is "IN" when it comes to Internet fraud. Law enforcement is urged to consider some of the suggestions in this article to reduce the cost, and hence, increase the likelihood of prosecuting Internet fraud crimes. At a minimum, prosecutors ought to consider a one-time full blown prosecution for deterrent effect on would-be fraudsters. Without some hard work on the part of law enforcement, consumer confidence in the safety of the Internet will only get worse.[126]

---

[126] Joris Evers, *Consumer Distrust Could Lash E-commerce*, ZDNET NEWS, Feb. 15, 2006, http://news.zdnet.com/2100-1009_22-6040075.html.

PANEL DISCUSSION III

WORKING WITH CORPORATIONS ON CASE INVESTIGATIONS

INTRODUCTION

Our third panel, coordinated by Hedda Litwin,[1] discussed the relationship between prosecutors and private industry in the context of cases involving Internet victimization.

Unlike the first two panels which focused on prepared questions and intermittent responses from the panelists, Panel 3 gave each panelist an opportunity to present information related to their particular employer or industry. This was followed by a more general dialogue that facilitated the exchange of ideas between industry and prosecutors. As such, what follows is the edited transcript of Panel 3 without a particular list of questions preceding it.

Marc M. Harrold[2]

---

[1] Cyber Crime Counsel, National Association of Attorneys General (NAAG).

[2] Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.

PANELISTS:[3]

- Jack Christin, Jr., Senior Regulatory Counsel, eBay, Inc.
- John Deerin, Vice President and Director of Security, Bank of Tampa
- Mike Robinson, U.S. Anti-Piracy Director, The Motion Picture Association of America
- Thomas Sadaka, of Counsel, Berger Singerman, former Assistant Statewide Prosecutor, Office of the Attorney General of Florida

JACK CHRISTIN: The defendant in this case got a rude awakening one morning from Lieutenant Dermot Quinn of the Massachusetts State Police who works at the Attorney General's office. The defendant sold four cars on eBay, but didn't deliver them. It was a classic non-delivery case, although it was substantial because it involved thousands of dollars. Four people in four different states bid on and won the cars, but they never got them.

We worked with the Attorney General's office and gave them all the information they needed to know about this defendant. While I don't know his current status, I know he was arrested and will be prosecuted.

I do want to touch on what we call the "scourge." I think I can speak for the panel that phishing and spoofing e-mails are a real headache for corporate America. It angers us because of what it does to our good names—whether it's Bank of America or a smaller bank such as Tampa Community Bank. In this case, it's the good names of Washington Mutual Bank and PayPal. Basically, phishers take our name and our logo and send out an e-mail which says, "You need to update your account with us. Go to this page," or "Put in your user ID and password, and we'll make sure that your account remains open." Of course, there's a link to a fraudulent spoof site.

---

[3] It should be made clear, at the outset, that the statements and opinions offered by the Panelists/moderator are solely their own and are not offered on behalf of any organization or agency.

We do a great deal of consumer education. We work with Digital PhishNet and law enforcement to try to stem the phishing problem. It still remains a problem because there are people out there who perhaps haven't been educated about these types of e-mails and who may fall victim to them. So it's a serious concern.

Here's an example of an eBay spoof site. Like other corporations, we ask anybody who gets a spoof e-mail to report it to us at spoof@ebay.com or spoof@paypal.com. We have a security team that works very hard with the ISPs and hosting sites to get these sites taken down. It's effective in a way because it gets them taken down. However, there are 100 other spoof sites going up every time you take one down.

So we're trying to work with law enforcement and other private entities to deal with this problem. We worked on a case involving spoofing and phishing with the Romanian authorities, the State Department and U.S. Customs. It was basically an Eastern European Internet fraud ring headquartered in Romania. They dealt in stolen credit cards and all sorts of stolen identity information, as well as spoof sites and spoof e-mails. Eleven people were arrested last year based on an investigation in which we, as well as other private organizations, provided assistance. I think it's a good example of how we work to stop phishing.

This case is placed at the top of our police blotter to send a signal to our community that we are working on this issue and that we do take it seriously. We can't just turn our backs on the phishing and spoofing problem. I think it's important for the private sector to make sure that law enforcement has the information they need to pursue these types of cases.

Finally, I think we're the only company that actually sends a survey to law enforcement to ask how we did when responding to their request for records. The scores could always be better, but they're usually in the high fours.

Basically, we want to know if you've had a problem reaching us, because we want to make it easier for you. If you weren't satisfied with the timeliness of the response of the FIT team, we want to know because we want these bad guys off our platform and prosecuted. There's no gray area here. We want them in jail, so we want to work with you to do that. We send out the survey to make sure that we're doing a good job.

We tell all our customers that we would never send them an e-mail which asks them to go to another web site. For example, we'll send a monthly billing summary from eBay showing the account activity, but it doesn't ask the user to go to another web site. It doesn't ask for any information. It's just a billing summary.

As much as you want to educate people and make them savvy, sometimes they then take a position that they're going to delete any e-mail from, for example, a Bank of America, PayPal or eBay. I think that's part of the reality of the phishing problem.

I don't have any statistics on the number of people who actually fall for these scams or the amount of financial damage it does to our companies in terms of loss to our members. When we think about corporation victimization, we tend to think of it in terms of our members being injured, not us. Obviously people may try to do harm to our platforms directly, but my focus is on our community members either being injured by another member or by somebody pretending to be us in the phishing/spoofing context. I don't know if there's a dollar figure. The problem is that a court may say, "Who lost money here? Who was financially injured?"

We've established a good relationship with the Romanian police because a good deal of phishing originates in Romania. Part of the problem is basically the jurisdictional challenges in dealing with another country. Obviously they have their own priorities in terms of law enforcement. It might not be a priority for them to go into an Internet café and take down phishers when they have violent crime on the street corner. However, they have been responsive because they know it's a problem. They understand that it's a serious threat to the health of the Internet worldwide. They're becoming a more modern country, so they've been very responsive. They worked on the case that I highlighted in conjunction with the State Department and Secret Service.

Digital PhishNet is a very good group. It's a consortium, and they share information and try to understand how we can work with law enforcement. Phishing and spoofing seem to be either international or federal, for the most part, but it's also happening in the United States.

Our first step is to get a phishing site down. We want our members to report the site to us. If we have information, we send it to law enforcement and basically say, "Here's a phishing case that needs to be pursued. It's a hot topic and needs to be addressed."

We have a very talented security team. They're very good at trying to trace e-mails but, like anybody else, we're limited in terms of our ability to do that. Sometimes it's based on how clever the perpetrators are. Sometimes it's based on resources. We have our contact information in a brochure, which also includes a detachable rolodex card. We're trying to make it as easy as possible for law enforcement to know how to contact our FIT team.

In 2002 eBay bought PayPal, so for the purposes of law enforcement, we're the same company. PayPal functions as a money transmitter, so many PayPal transactions have nothing to do with eBay. In terms of eBay, about 95 percent of eBay listings offer PayPal as a payment service, so if law enforcement is dealing with an eBay fraud case, there's a strong likelihood that PayPal will be involved as well.

Providing useful victim information to a law enforcement agency that is investigating fraudulent behavior by someone involving eBay and PayPal is key to our commitment to fight fraud by assisting law enforcement. We will search both PayPal and eBay records at law enforcement's request and will determine the identifies of the victims for the agency involved. We will also disclose the name of any agency with which a victim has filed a complaint, whether they contacted an Attorney General's office, the Internet Crime Complaint Center or any other law enforcement entity. We will give all of that information to law enforcement so that it will help in building the case.

We have a Security and Resolutions Center is on eBay.com, with a prominent link to the Center at the bottom of every page on the eBay site. I urge everyone to take a look at it. It has a law enforcement page that addresses how to contact us. I also have a colorful two-page brochure which summarizes the information available to law enforcement from eBay and PayPal, as well as how to get it and how long it takes for us to send it. If just basic identifying information for a seller is needed, we can probably get that to law enforcement in three days. If it's a total listing history and PayPal history for a member, that might take two weeks. It just depends on the volume of requests that we're getting and how badly the information is needed. If it's really needed in a week, call me or the FIT team, and we'll do everything we can to get it. This is one-stop shopping on how to get information from us and what can be expected in terms of the timing.

This discussion is somewhat of a law enforcement DNA of eBay and PayPal. Since we knew that we were going to have relationships with law enforcement, we knew it was important to have former law enforcement people on the team. As an example, we have on our team a former member of the Australian police; we have a former investigator from Scotland Yard; and we have several former Assistant U.S. Attorneys. I think it gives us a culture of understanding of the challenges that law enforcement faces. We literally have been there in investigating these types of cases, so we can be sensitive to law enforcement's needs, and we can make sure that we work with law enforcement and that law enforcement gets what is needed from us.

For example, if one wants to get the Ohio Attorney General's attention, one way to do it is to sell $60,000 worth of Ohio State football tickets on eBay and not deliver them. Last fall when Ohio State played Michigan, Mark West posted several listings for tickets. People bought them; he never delivered them. He took off to Florida. EBay got complaints, such as, "I didn't get my tickets. The game is in three days. He told me he'd have them to me a week before the game." As we got complaints, we saw a pattern of behavior by this eBay user ID that concerned us. We called the Ohio Attorney

General's office, which is another example of the FIT team being proactive with internal information. They were already investigating the situation and preparing a request to us for information. However, we called them and said, "We've got a seller who we think is in Ohio. He's selling Ohio State football tickets." We were able to get them information. West just took off for Florida and was on the run for two months. He was arrested at a bar in Florida in mid-January and is now awaiting trial. The Attorney General's office is handling that case.

Here is another example of how we work with both federal and state law enforcement. Jeff Lee was selling pirated DVDs. The Ashland, Massachusetts Police Department got a tip that a person was coming into his local post office about five times a day and getting an unusual amount of packages from China. The post office thought it was suspicious and thought the police might want to investigate. The police theorized that he was getting pirated DVDs, which turned out to be true. He was selling them both online and offline. He was listing many of them on eBay. U.S. Customs in Boston contacted us with a fax request. We sent them all the basic fax request information. They developed the case and realized that he was a serious seller of pirated DVDs. Two weeks later, they subpoenaed us for his entire eBay history-everything involving PayPal. We gave them all the records pertaining to Jeff Lee. He's currently awaiting trial on these charges.

MIKE ROBINSON: Movie piracy is not just about actors, actresses and directors. It's about hundreds of thousands of people in every imaginable walk of life who are associated with and who make their living as part of the film and movie industry.

So it's not just the actors that are losing out because of movie piracy, it is truck drivers; it is painters; it is electricians; and it is seamstresses who are hurt by it. Of course, it's about actors and actresses-creative talents who want to get their artistry out in front of the public. However, at the end of the day, it's also about paying your bills and putting enough food on the table.

I think many pirates or the public in general have the conception that movie piracy is doing a service to these artists because they're getting more people to see them on screen. They think that it is a good thing, but it's not. The fact of the matter is that piracy is big business and is becoming more sophisticated. Pirates are smart, well-organized and well-funded. They also use their funds to perpetrate other crimes against us and the public.

So how does piracy occur? It's very rare that we lose money when a movie is in production, but you can almost guarantee that as soon as the movie hits the theater, it will be stolen. It will be stolen in this country by someone in the theater recording it with a camcorder. You may think, "Who would buy one of those movies recorded with a camcorder?" Frankly, they buy them because of the sophistication of camcorders and their ability to record movies with good quality in a theater. Now that they tie into sound systems for the hearing impaired, they also get a good soundtrack.

We track movie theft. When we have a movie that was recorded by a camcorder in a theater, we can track that back to the specific theater where it was recorded. That's because studios watermark all of their films and mark them differently, so you know the exhibitor who got a particular copy of a movie. You can say, "This was recorded by a camcorder at Cinema 12," and that's very helpful.

We don't lose many movies during the marketing phase. All movies are rated by the Academy of Motion Picture Arts and Sciences for awards purposes. We also don't lose many movies in non-theatrical efforts. However, we lose them just as soon as they are released on DVD.

The problem that we have with films that make it to theaters, both in this country and around the world, occurs when they are shown. The theaters receive normal reels of film, generally about eight to a movie. As the industry moves toward digital technology, and theaters move from reels to digital showings, it will obviously compound our problem.

There are generally two kinds of pyramids to the piracy problem that we address. First we look at the online side-the release groups that get the material and send it to the consumer through peer-to-peer networking. Then we look at the side that we call hard goods, where they actually duplicate movies and put them out on the street through couriers and distribution networks. It is very similar to what drug traffickers might do in a distribution network to get drugs out for sale.

I'm going to focus my remarks on that pyramid on the left side—the Internet side of the problem. There is a great deal of sharing of content back and forth as we move down those streams. Where we're beginning to see more problems is in the online sales of pirated goods through web sites that are set up just for that purpose. I'm going to talk about two things. I'll talk about the method by which these encoding groups get the films to the peer-to-peer groups. I'll also talk about the pirate web sites on the Internet and the actions we're taking against them.

These groups are very sophisticated and bold. They actually try to recruit people who are in the movie business. These are the people who remain at the very top of that left pyramid, and these are the people who are getting a copy of the film, either in this country through a camcording or a DVD release of that movie, or from another country through a showing and release. They often put the film together with an audio track from another country, or they put it together with several audio tracks in different languages for redistribution around the world. This can be done in a matter of hours.

These groups are very sophisticated, and they're very small. They may contain only six or a dozen people. While they may never meet one another physically, they've met one another over the Internet and through chat rooms. They do their research about one another. You have to get into one of these groups through references and other connections. It's a very sophisticated and difficult operation.

We have within the Worldwide Anti-Piracy Office an Internet piracy program that tracks and investigates this type of activity on an international basis. The United States program also has Internet software that studies the crimes that are being perpetrated in the United States. Since the Internet knows no international or state borders, these investigations are obviously very difficult to conduct.

The perpetrators move the copies after they have synchronized them with audio or stripped off the watermarks. They're getting more sophisticated at stripping off the watermarks or stripping away the protections that we have on DVDs. Then they push the films out to their sites and then rapidly onto peer-to-peer sharing networks. You then have millions of people able to access that material, in many cases within a matter of minutes.

The studios really rely on what they call their "tent-pole productions,"—the movies that they are going to make and that are going to carry them through the year. For example, "The Chronicles of Narnia" and "Mission Impossible III" are coming out. We watch very closely to see how rapidly those movies are stolen and how rapidly that material ends up on the street.

These groups even rank themselves as to how good they are. They openly brag about how well they have conducted their business. A television showing of, for example, "24" on the East Coast will be encoded, downloaded and available on the West Coast within minutes after its completion.

The groups use IRC channels and also specific sites: eDonkey, eMule and BitTorrent. Since I came on board at the Motion Picture Association, we have taken a BitTorrent operation down in Sweden that had millions of users associated with it.

Obviously, these people are much more sophisticated than the average Joe. The average Joe might be able to put 50 movies on his system, but these other systems may have as many as 10,000 movies available for peer-to-peer distribution and downloading. It's a serious issue.

The other serious problem is that we find some of these top sites are actually housed within corporate America. That's due to the fact that if you get into these systems and see the advertising, and if you have large system capacity, you can set up within a corporate system where you have control, or you can plug into a university or corporate system. We find many problems here because of that capacity.

There are piracy web sites, and the average person really can't tell that these sites are marketing bad CDs. However, there are some tell-tale signs. The movies they're marketing are still in theaters, and they use different selling prices which are tied to the quality of the DVDs that they market. They also have bad grammar because many of these sites are outside of the United States, and so the language translation is not always as smooth as it should be. Another sign is that you have no physical address if you want to get back to them.

The MPAA sends out thousands of letters every week to ISPs about sites that we have identified as problems to us and that should be taken down. I have to commend eBay and PayPal because they have been fantastic in assisting the Motion Picture Association. For that matter, they have been very responsive when we have identified someone on their system who is dealing or marketing pirated movies and music, as we work very closely with the Recording Industry of America as well. They help by closing the PayPal accounts of these pirates. The average person who goes to one of these pirate web sites sees that they can pay by Visa, MasterCard or PayPal, and that adds another sense of respectability to that site. The assumption then is that it must be okay or these sites would not be allowed to use Visa or MasterCard. I wish that was the case. We have had much better luck with PayPal and eBay than with some others in shutting down their accounts and systems.

Here are some of the questions that concern us. Are there ISP sites operating which are nothing more than pirate havens? If so, are they set up the same way as some flea markets or swap meets, or are they like some buildings in New York City which only house dealers of counterfeit goods? Is it only another marketplace for these goods? We're looking into that right now. As we identify targets that have a consistent problem, or that continue to deal in these goods, we may come to law enforcement for assistance.

We're working on some cases, such as in New York City.

The Motion Picture Association, the recording industry, Louis Vuitton and other brand owners have been into some buildings on Broadway in New York City with law enforcement time and time again, and yet they continue to operate. The owners and landlords of those buildings continue to allow pirating activity to occur. We need to investigate those building owners and perhaps put them out of business, instead of only investigating the marketers within those buildings.

It's the same way with those ISP sites. If we identify certain ISPs that are consistently a problem, there are people at those ISPs who we will want to go after, and we will ask law enforcement to help us.

How profitable is piracy? Why would you want to run a methamphetamine lab with the danger of blowing yourself up, or with the smell that makes it easy to be caught, or the penalties associated with that crime, when you can make more money with less risk by setting up a DVD burning tower in your bathroom? Well, guess what? Some people have asked themselves that question, and they've come up with the "more money less risk" answer. We're seeing gangs and other organized criminals migrate to movie and music piracy as a way to fund their other criminal activities. It's been a consistent and frightening pattern because we've had some serious threats made against our employees in other counties. We've also seen serious threats made against law enforcement people who have engaged in investigating these cases.

So it's a serious problem for all of us. There is also a link to terrorism. I believe there was an indictment unsealed recently in Michigan about a terrorist connection to pirated cigarettes and other illegal activities in the Dearborn area. The investigation on that case actually started while I was the State Police Director in Michigan. We worked with federal law enforcement agencies on it. After I came to MPAA, I saw that those same people we investigated in Michigan are now engaged in movie piracy as well, so there is a connection with terrorism. Piracy is not a harmless crime. It's not a crime that any of us can turn away from and consider as a minor offense.

One of my objectives in coming to MPAA is to convince law enforcement that when they drive down the street and see someone selling pirated movies, they don't say to themselves, "Oh well, at least he isn't selling crack," and drive away. Piracy is a crime that's connected to terrorist activity, and we have to do something about it.

Obviously we can't do it without law enforcement's help. After 40 years of public service, I know what its like to be in law enforcement's shoes. I know what it's like to have tight budgets and plenty of work and to not always have the resources needed to get it done. While we can't do the job without law enforcement, there are some things we can do to help on these investigations. We do research and analysis every time we see a new title that has been pirated, every time we see that title in another location and every time we see it in another country or state. We sample copies of disks. There are two ways of copying a disk. One way is by duplicating it by going through a presser machine. We take samples and exemplars from all of the pressing equipment around the world.

JOHN DEERIN: From a case management standpoint, the financial security business hasn't come very far. We continue to work on it, but the large banks are much more involved than the small banks. From a criminal referral standpoint, there are no dramatic improvements in working with law enforcement and referring cases. Here and there, we do things a little better.

How big is the problem? You hear astounding numbers put forth. I heard a number from an international security expert a month ago who said financial fraud is a three trillion dollar business worldwide. How do you come up with these numbers? How does someone calculate three trillion dollars? Could it be $2.5 trillion? Could it be $3.2 trillion? Let's just all agree that we know it's a big number. When you talk about fraud, it takes on so many aspects and makes a huge impact.

We take significant, hard losses that threaten our reputation. It's not just the corporate entities that take those losses. Those losses eventually are passed back to the consumers.

In the banking and financial industry, it's very sexy to talk about Internet fraud. However, counterfeit check fraud is really hurting banks. One bank recently returned $803,000 in counterfeit checks during a one-month period. Another bank reported $1.2 million in counterfeit Canadian checks that had been deposited into United States accounts, again just in one month. These are statistics that I got from the American Banking Association recently. The numbers are incredible. One bank reported a 2,000 percent increase in check fraud between 2000 and 2005. These numbers tell us we need to do better. We need to do things differently. We need to "step out of the box" and figure out what's going on.

Who's the victim in the banking business? The victim is either the bank, which takes the "hit," or the customer who doesn't get the money back from the bank. Everything is about claims. The customer will eventually go to the bank and say, "Someone made this unauthorized transaction for $700 against my credit card or against my bank account. I want my money back." Most of the time, the bank will have to give them their money back. However, many times, particularly as it relates to check fraud, the bank will utilize numerous defenses under the Uniform Commercial Code, and will not give the customer their money back.

For law enforcement, there's a learning curve as to the identity of the real victim. The financial institution is a victim because if the customer must be reimbursed, the institution has to give them the money back. The customer is the victim if the financial institution denies the claim for reimbursement and the financial loss is shifted back to the customer. The victim is also the customer if he or she has been swindled or duped and has sent authorized funds to the fraud perpetrators. The bank is not going to take that loss.

The victim can also be both the bank and the customer if they've both been duped by some sort of phishing scam and have sent the money themselves. If the bank has paid that debit or check, and the account is now overdrawn by $4,000, the bank is out $4,000. The bank will pursue the customer to get that money back.

How are fraud schemes reported? Victims generally have little knowledge of, or the ability to properly report, these crimes. Often the actual crime will be outside of the jurisdiction, and the victims will clearly be frustrated, both with the banks and with law enforcement as to what they need to do.

Some financial institutions have very well organized fraud departments. They're very effective in helping customers in fraud situations and directing them in the right places. However, many of the medium and smaller sized banks, and even some of the large banks, don't have good programs to ease their customers through these frustrations. Financial institutions will vary greatly in their ability and effectiveness to report these crimes. Some of the fraud departments in big banks work very closely with law enforcement, so they can be effective.

Many banks don't even have security departments, or even full-time security people, so they obviously won't have a knowledge base of what they or a customer needs to do in a fraud situation.

Many of the larger financial institutions, by the way, utilize very significant thresholds, and they won't even get involved in a case unless it's over $5,000 or $10,000. Obviously they'll take a look at the circumstances, but it's very difficult to develop fraud suspects, and the criminals know it. If it's under their particular threshold, they just simply don't have the ability to handle the case, and they'll charge it off and walk away from it.

The mechanism by which financial institutions are required to report crimes is through the suspicious activity report, or SAR. It is required by the banks' regulator to be filed with FinCEN, the Financial Crimes Enforcement Network, if there is a suspected crime with a loss exposure greater than $5,000 and a suspect has been identified, or a loss exposure of $25,000 and a suspect has not been identified. I can tell you that this law is loosely followed. First, there's a nebulous nature to loss exposure, so many of the large banks, unless it's a hard loss of over $25,000, may not complete a SAR on it. Many of the smaller banks probably are more diligent.

We file thousands of SAR reports electronically to

FinCEN, and then FinCEN redirects them back to the applicable federal agency, whether it's the Secret Service, the FBI, ICE or another agency. The agency will have its own intake process when they review these. As we know, a U.S. Attorney will not pick up the case for prosecution, or won't do much about it, if it's not over a "gajillion" dollars. That's the way the SARs work. You have to remember that these are only for fairly significant cases. The numbers don't include all the $800 or $3700 counterfeit check fraud and credit or debit card cases. These files alone represent fairly large loss numbers.

There has been a significant increase in the number of SARs since 2001. That increase was specifically related to September 11 when the government told banks that they needed to do a better job of monitoring cash activity and the money laundering potential. Banks obviously began to comply more than they had done previously and started overfiling these SARs. In 2004, banks filed 381,000 SARs, but in 2005 the backlog was so large that the government backed off a bit. Now you see that money service businesses, which include check cashers and other like businesses, are required to report SARs.

I'm told that the SAR database will be made available to state law enforcement. I believe that in some states it may already be available for data mining by state law enforcement. The proviso is that from a fraud standpoint the information in the SAR may not be relative to an investigation or case. However, it's certainly a resource to review.

A good point was recently made that while financial institutions spend so much time preparing these SARs, and rarely will they receive contact back from law enforcement to say that they've looked at or are working on this SAR. It's always good for law enforcement agencies and prosecutors to work closely with the company, whether it is a financial institution or another entity, which has reported a crime to them. Even if a decision to prosecute hasn't been made, it gives the entity a feeling that their actions have done something as opposed to just going into a black hole.

Where does all the money go? We know about the day-today street level activity. Counterfeit check fraud, for instance, often goes just to support street level drug habits or lifestyles. We know that the large dollar financial crime has certainly been associated with international terrorist activity, particularly the large amounts of financial fraud in Florida in the early 1990s.

It's a systemic problem. Financial institutions for too long have just charged losses off, and it still continues with little or no effort to productively pursue the perpetrators. We charge losses off too quickly. For example, if you call American Express and say, "I didn't make this charge," it's off your account in two minutes and charged off. We just have to take more ownership of the problem.

That's one problem. Low to mid-level white collar crime generally brings minimal punishment compared to other crimes, so the low to mid-level perpetrator sees substantial and immediate reward with low risks. For us, it's a bad combination. The banks are quickly walking away from it. Secondly, on the prosecution side, the statutes, particularly the lower level statutes covering such things as check fraud, carry insignificant penalties.

A large financial institution even today will charge off, for instance, $30 to $40 million in their state alone in check fraud. That's how big the numbers are. Approximately $40 million a year in the state of Florida alone has been charged off to what they call "non-credit losses." A large portion of that is fraud-related; more specifically, check fraud.

When I first started as a credit card fraud investigator, fraud losses were less than one percent of your credit card portfolio. That was considered to be tolerable. The actual collection or the charge-off or delinquency number was about three percent. Now three percent is considered tolerable for fraud losses and five or six percent is tolerable for credit losses. There is just too much tolerance of these kinds of losses.

What are we doing about it? Prevention is the absolute key as opposed to chasing after it. We are continuing to develop banking industry systems to detect fraud early on. The artificial intelligence type of systems try to evaluate a customer's activity, and if the activity falls outside of the parameters, the customer will be contacted. We're doing better. There's a reconciliation system and the more the bank can sell that, the more they can help their customers. Right now the benefit is on the business side. Businesses will send in their issue file, or all the checks that they've issued that particular day. When the checks come in to clear through the bank, they will reconcile them against one another. Those are the kind of things that are going on to prevent losses.

We have to do a better job of making our customers aware of the scams and advise them not to enter their pin number on a phishing site that asks for their bank account information or pin number. That's a critical area in which banks and the government have to do better.

We try to work with law enforcement. We try to recover the money while it's still in the stream and trace the losses. We win some battles, but we're probably not winning the war.

When bank security folks get together, we always tell each other that if we could identify the top ten perpetrators, and we could get law enforcement and prosecutors to take them out, we could reduce 60 or 70 percent of the fraud that's occurring. We haven't been able to do that. I think we need to look more at identifying those top ten players and try to maximize the penalties on them when they are prosecuted. How successful has prosecution been? It's been occasional and sporadic. Many times, a defendant, particularly in check fraud operations, is recruited by the leaders of the organized rings. It's really hard to get to those key perpetrators.

Jurisdiction is the number one barrier. I think we need more permanently established task forces to deal with this multi-jurisdiction activity. We have too many police departments and law enforcement agencies. It's very frustrating for banks and customers. There are twenty law enforcement agencies the nearest two counties to my bank. There are staffing inefficiencies at both financial institutions and law enforcement. Sometimes we've had a $20,000 fraud case with good evidence that we've been trying to refer to a police department. It'll just sit there, and the police won't do anything. You get very frustrated. Then you'll get a detective who will call you about his case about a $300 check that was cashed. It just doesn't make any sense. I guess there's an obligation on their part to take the cases as they get them, but we just need them to do better and attack the big cases.

Is there anything else we can do? We need to manage our cases better, both on the bank side and on the law enforcement side. We really need to attack these cases in a more organized and efficient way instead of chasing $300 checks when we have a $20,000 case over here. We need to prioritize. We need to utilize information- sharing databases, like the SAR database. Prosecutors need to share intelligence information on these bad guys to try to determine the identities of the top ten players and go after them.

Fraud-Net was actually established in Florida and then adopted first by the Florida Bankers' Association and then by the American Bankers' Association. It has become fairly successful in Florida. Both the Tampa Bay and Miami Dade regions, for example, have their own grouping. When they click on the Fraud-Net site, they will see listings of all the alerts, organized by the type of fraud or crime, such as check fraud or ATM/debit card fraud. It really is a great tool with which to share information between the private sector, financial institutions and law enforcement. It also has a directory where law enforcement can find the bank or the contact they need, or one can go on the law enforcement side and find out who's working on economic crime at that particular agency. It's been very helpful.

I would recommend that prosecutors identify and focus on organized activity within local and regional jurisdictions. Reconsider the multi-agency task force. I'm sure that many Attorneys General are trying to get their legislature to increase the penalties on these crimes.

We haven't seen the breaches of computer systems that many of us have been lead to believe have occurred. Most of the crimes that financial institutions face concern check fraud and counterfeit credit cards.

MIKE ROBINSON: Training for law enforcement is extremely important to us, whether it be for high-tech task forces, beat cops or other organized crime investigators. We would like to do more training with prosecutors and courts, quite honestly so that they understand the significance of the problem.

We do a great deal of the investigation ourselves before taking a case to law enforcement. We work through a network of over 100 private investigating firms in the country that we monitor very closely. They work on our behalf and have been very productive.

We'll provide some legal support as well. One ongoing project that we have goes through cases to develop some case history for law enforcement, so if we get a call from a prosecutor with a specific concern about a case, we can relay information about cases that have been adjudicated in other jurisdictions as well as contact information within those offices.

Public relations and public education are extremely important to us. We have a very aggressive program now that is targeting colleges and universities because a lot of activity is going on there. We also have an outreach program for school-aged children which tries to educate young people before they get involved in this illegal activity. We're here to assist in any way that we can.

We're working on a report right now that indicates that every business where cash money is handled has the potential for illegal activity. whether it's cigarettes or handbags or movies. We want to verify the facts that are reported in print in congressional testimony and other locations before the report is released.

We work very closely with the Recording Industry Association of America because there isn't a single location we go into that is selling movies that isn't also selling pirated music. We actually have three joint offices with the RIAA in Miami, Atlanta and Chicago, and we are about to open a fourth office in Boston.

The United States Chamber of Commerce has become very aggressive on behalf of their members where violations of intellectual property rights are concerned. We're working with them and their membership so that we're not all running after law enforcement or prosecutors and pulling you in different directions when we all have the same goal in mind. You'll see us doing more of that work together. We're about to start a very aggressive effort in the Southwest border states in regard to counterfeit goods and property that are entering the United States and then being shipped to other locations. So again, we appreciate your help.

MPAA has offices in Washington D.C. where our state outreach program is managed by Vance Stevenson. He's worked with states across the country to get state statutes enacted and to increase penalties for those crimes and move them from misdemeanors to felonies. I think there are only five states where we do not have an active program right now.

One other thing we do for prosecutors and law enforcement is that we can get the necessary records from the studio-the owner of that property – and they may possibly be available to testify on the value of the loss. That's a difficult thing for us to put together, but we will do that.

JOHN DEERIN: I've been in the financial security business for almost twenty years. Before that, I was a beat cop for ten years. Then I worked for Barnett Bank, which became Nations Bank, which then became Bank of America, for 15 years. So I have worked in the corporate security group of the "as big as you can get" bank situation.

Then in 2002, I got a call from this local community bank which was also the 12th largest community bank in Florida, located in Tampa. I joined them, and now I'm working in the community, which really represents a much greater number of the banks that you would deal with on a daily basis.

So I've worked on both sides of the financial security business, and each gives you a different perspective. As a matter of fact, when I left Bank of America in 2002, we had 350 employees in our corporate security group. At the Bank of Tampa, we only have one, but it's kind of fun.

JACK CHRISTIN: I came to eBay in 2004 from the Attorney General's office. Basically, my job at eBay is to be law enforcement's point of contact for any questions or concerns about things that you see on eBay, whether it be about sellers, buyers or the PayPal platform.

Our Fraud Investigation Team, or FIT, members investigate fraud on the eBay platform. This is a very dedicated group of about 20 individuals located in San Jose and Salt Lake City. Their job is to respond to law enforcement requests for information, whether it be by informal letterhead fax request, a subpoena or a search warrant. They have the tools to go into our systems and get everything needed by investigators and prosecutors to bring a case.

FIT doesn't just do responsive work. FIT actually does a good deal of proactive work in terms of taking referrals from inside the eBay or PayPal companies and from sources other than law enforcement and trying to detect and identify fraudulent behavior that involves our platforms. In many cases, they refer a case to Attorney General offices rather than just reacting to requests.

FIT investigators also will testify in court to support your cases. In other words, they will do whatever they can to support investigations that involve eBay and PayPal. It essentially tells our community, "We will work with law enforcement and share information with law enforcement where appropriate—not third-parties or private corporations—but law enforcement agencies. If we get a verified request from law enforcement on their letterhead asking for information as part of an investigation, we will share basic information with them about you and about your conduct on eBay. If they need more information like credit card numbers or Internet protocol data, we will require a subpoena. We'll give them basic information to help them at least initially start their case."

Regarding PayPal records, anything that you need on the PayPal side requires a subpoena. PayPal is a money transmitter service, and thus involves our members' financial information. In that case, contact me or the FIT team, and you can get it from us by subpoena.

JOHN DEERIN: When I was a credit card investigator, Visa and MasterCard told us in the early 1990s that credit card fraud would be eradicated by 1995 because they had holograms to put on the credit cards as well as more security features. The skimming is what we hear about — whether you go to the restaurant or whether you use your card at a gas pump. Those dollars skimmed are significant.

Right now the emphasis is on money laundering. If a bank has suspicious money laundering cash activity, it's required to complete a SAR. There's a strong emphasis, as well there should be, on stopping money laundering, so a great portion of SAR filings are on that situation. As far as actual crimes are concerned — whether it's bank fraud, check fraud or credit-unless the crime meets those thresholds, a SAR report may not be made.

How many reports are actually picked up for further investigation and prosecution? I can only tell you that we never hear back on any of them, and I file hundreds of SAR reports. I don't recall ever getting a callback from a federal agent or prosecutor about a case.

TOM SADAKA: If I were to tell you how to streamline your case management and your investigative process into a "bundle" that is readily prosecutable with very little more work that's required either from the investigative side or the prosecutive side, could we do business today? The "bundles" that are put together by the financial fraud investigators at the larger and even the smaller banks are incredible pieces of investigative work. These individuals are often former trained law enforcement officers. They have access to information within the bank that you could access only with four or five different layers of legal process. They are able to use that information in the development of these investigative reports.

I talked to the head of security at a credit card security conference who told me they can spot a skimmed credit card within three uses and shut it down. So I said, "It would be wonderful if we could have a joint relationship between government and you as the private sector." He was very much in favor of trying to develop some type of task force or working agreement with prosecutors and law enforcement. He immediately talked to their vice president in charge of marketing, who said they wouldn't be interested.

Their loss was $1.4 billion a year. Don't you think that they'd be interested in doing something when their loss was that high? However, it was a pittance compared to the amount of revenue they had. In further drilling down through the system, they wouldn't be interested because they have little faith in the ability or the willingness of law enforcement and prosecutors to take the investigations in which they participated and prosecute them.

Historically, they had a reason for that. They got very little response from prosecutors when they tried to get these types of cases prosecuted. I hope I am preaching to the choir that we can't handle these cases without the cooperation of the private sector. What better way than through an organized task force or through a relationship with these various institutions, whether it's eBay, MPAA or a financial institution such as Bank of America or the Bank of Tampa.

I can tell you from personal experience that I've dealt with each of these organizations, and I had glowing praise for them. EBay is incredible. MPAA is willing to put someone on the next plane to fly down to train an investigator on how to work this case. Bank of America handed me an investigation that they had been working on for several years that saved us probably a year and a half worth of investigation and resulted in a conviction of a $13 million identify theft ring based in Miami. It was the Campbell case.

We were able to bring their investigators and their investigative packet before the grand jury and get an indictment with very little involvement of law enforcement. We had a statewide taskforce that was in place that focused primarily on identity theft, so we developed this relationship.

What happened to that task force? As many of you know, law enforcement relies on many positions, such as our community crime investigator or our financial fraud investigator, but the longevity of those positions is rather short- lived. Why?

The computer experts usually go to the private sector where they can make more money. The rest become career law enforcement officers. However, for those of you who understand how sheriff's departments, state police and local agencies work, is the fraud investigator going to be the next captain? Generally not, isn't that right? Instead, he will become a road supervisor or lieutenant. He'll end up in violent crime and then he'll get a position under the sheriff. You will not see the fraud investigator running for sheriff. I'm offended. I'm a fraud investigator. Why is that not a career position? We see it in prosecutor's offices. If you have a well-trained computer crime investigator, they end up getting moved or promoted into another division that deals with sex crimes or other violent crimes.

We need institutional memory. How do you accomplish that except through a task force or some type of joint cooperative effort between the public and the private sector? That taskforce has enough overlap and longevity to remember a specific case. They remember an investigation that might have gone stale. They remember how things were done in the past that were successful. That's really what we need to focus on.

MIKE ROBINSON: Before I joined the TSA, I spent 34 years with the Michigan Department of State Police. Most of that time was spent on the criminal investigative side of the operation as director of the Michigan State Police for nearly 12 years. During that time, I served as the president of the International Association of Chiefs of Police, which really helped me in my current job because it certainly requires a great deal of cooperation between the industry and law enforcement around the world.

I think that there's a misconception held by most people that the movie industry is all about making money. The fact is that the movie industry is as fragile as any other industry in the United States or internationally. Only a few movies ever really make money, and the studios hope that those blockbusters carry them through the rest of the year.

I learned as soon as I left my badge and ID in Michigan and got into the private sector that there are things law enforcement can do that we in the private sector cannot do. We absolutely need your help. We absolutely need to work cases with you in order to achieve our goals as well. We can't do it without the tools that you have in your toolkit that we don't have.

JOHN DEERIN: The chargeback process is the first step in any type of credit card fraud. Banks are going to take their chargeback rights. It shifts the loss back to whoever accepted that credit card, whether they can get authorization or whether it was an online transaction that wasn't verified through Visa. I'm sure it complicates matters from a prosecution standpoint. The chargeback system has been in place forever and always will be as a recovery methodology.

When I was at Bank of America, we'd get many restitution checks per month in our Tampa office, and they'd all be for amounts such as $27, $18, $22. Restitution is almost a non-event from a recovery standpoint, unless it's a big prosecution case where we're able to get big money in return. The restitution checks at $26 a month don't get them excited.

TOM SADAKA: Frankly, you can't have a financial crime without technology being involved. When you're working with task forces, you have a combination of efforts and talents that will allow you to work these cases successfully.

Every prosecutor knows the Electronic Communications Privacy Act. What does it do for you? It gives you, as a government entity or official, a roadmap on how to get certain information from a provider of electronic communications. Do you have any idea how the people in the private sector can get that same information?

That was a rude awakening for me when I left government service. I had a public company as a client that was dealing with very negative postings about the company in a Yahoo! group. The poster had enough inside information about the company to legitimize what he was saying. It was all untrue. How do you get that information from Yahoo! if you're not a government entity? I couldn't send them a subpoena without filing suit. Could I file suit if I didn't know who it was? Procedurally, I could file a John Doe suit and get the subpoenas required to get the basic information. Then I might have to send another subpoena to find out the IP information and another subpoena to the individual's ISP to find out the identity of that person. So when the client asks how much that is going to cost, it might be as much as ten grand in legal fees. If we file suit, it will probably cost the client $100,000.

You have a statute that procedurally allows you to follow through. My purpose in discussing this is that when the private sector comes to you for help, and you find probable cause to predicate your investigation, don't look a gift horse in the mouth when they're presenting you with the investigative packet. Also, there may be a legitimate need, and that little case may turn into something big. That case may not be a good example of anything other than to show you that it's difficult to get that information, but in a single online fraud case, there may be something else brewing beneath the surface.

I just encourage you to maintain relationships with the private sector and try to foster task forces. If there are ones that already exist, get involved with them if you aren't already. If there's somebody else in your agency who is involved but isn't really handling those kinds of cases, perhaps it's time for you to come forward and supplant that person within the task force. You may be amazed at the results.

JOHN DEERIN: I want to clarify that it's not that we don't care about restitution, because banks want to prosecute these criminals. From a bottom line standpoint, particularly at the Bank of Americas of the world, they may charge off $40 million. This is their strategy. If you've got a $20,000 credit card fraud, and you can effectively chargeback $10,000 of it, that will be your first course of action. At the Bank of Tampa, if you have a $3,000 check fraud case, and you work out a restitution agreement of $100 a month, it's greatly appreciated. You can only imagine what that $100 check means to

Bank of America. However, if a victim has a $200 bad check, that's the same to them as when Bank of America has s $100,000 fraud. Police departments can be in a quandary because they can't decide to work the $100,000 fraud and not work on all the smaller citizens' cases.

If a bank is not taking a hard dollar loss, they simply don't have the resources to pursue it. It's very frustrating to our customers because they don't understand, even when they're not out the money either, they've been violated.

TOM SADAKA: In an identity theft, the bank doesn't consider itself a victim, but we still have a victim—that individual whose information was used. Now the bank is a witness in that case, and you can rely on whatever investigative information they have. If you have a task force, such as we have with the Florida Bankers' Association, prosecutors can go to them to work together. I know that their security people would love to see these cases handled, but not the marketing people. You should work that as a point of communication between you and the financial institutions.

JOHN DEERIN: Some small banks, such as mine, have insurance on their credit portfolios, including their credit card portfolios through their credit card processor and other associations of which they're members, such as the Credit Union Association or, in our case, the Community Bankers' Association. This insurance has a deductible, but then you get 50 percent on your losses over that amount.

The realities of the banking industry are that there's all kinds of internal theft possible. The big banks have huge internal call centers, with 500 to 600 people who have unlimited access. They try some front-end proactive approaches to analyzing who is looking at what information and what they're doing with it. At the end of the day, the volumes of those transactions that these folks are handling are great. Their capabilities are significant.

SENTENCING POLICY AND PROCEDURE AS APPLIED TO CYBER CRIMES: A CALL FOR RECONSIDERATION AND DIALOGUE

Donald R. Mason[*]

I am very pleased that we have devoted the concluding half day of this conference to topics relating to the intersection of sentencing and Internet victimization.[1] This is of very special interest to me because I teach courses in both cyber crime and sentencing here at the University of Mississippi School of Law.

I. SENTENCING REGIMES AFTER *BOOKER*

Within the last three years, the United States Supreme Court has dramatically shifted the landscape of sentencing law. In *Blakely v. Washington,*[2] the U.S. Supreme Court ruled the State of Washington's sentencing guidelines were unconstitutional because they allowed a judge to enhance criminal sentences based on facts not determined by a jury or admitted by a defendant. Constitutionality of the Federal Guidelines, similar to Washington's, were called into question. In *United States v. Booker,*[3] the Court extended the *Blakely* rationale to the Federal Sentencing Guidelines and rendered those guidelines advisory. Although *Booker* concerns the right to a trial by jury, the decision has significant ramifications for the policy and law of sentencing.

---

[*] Associate Director of the National Center for Justice and the Rule of Law at the University of Mississippi School of Law. Prior to joining the NCJRL, Mason served as Senior Legal Research and Training Attorney for the National White Collar Crime Center, developing and presenting legal training on computer crime, computer related criminal investigations, and other white collar crime topics. Mason began his legal career as a prosecuting attorney in his native state of Iowa. He then served for twelve years as the Iowa Prosecuting Attorneys Training Coordinator and Executive Director of the Iowa County Attorneys Association, coordinating statewide training, technical assistance, and governmental liaison.

[1] Remarks at the Conference on Prosecutorial Responses to Internet Victimization. The conference was conducted at the University of Mississippi School of Law under the partnership of the National Center for Justice and the Rule of Law and the National Association of Attorney Generals April 4 through 6, 2006.

[2] Blakely v. Washington, 542 U.S. 296 (2004).

Although this training conference is intended for state prosecutors, a review of the changes in the law and policy behind the Federal Sentencing Guidelines is relevant for several reasons. First, the Federal Guidelines, rightly or wrongly, are the "800-pound gorilla" in the room. The federal government prosecutes more crimes than any individual state in the area of cyber crime, and thus generates the most case law and commentary on the nexus between cyber crime and sentencing policy. Second, because many states have sentencing schemes similar to the ones invalidated in *Blakely* and *Booker*, federal precedent affects approximately one third of all states directly. *Booker* also affects all states indirectly to the extent the Supreme Court addressed constitutional issues in sentencing. Third, the rationales expressed in federal cases, particularly landmark cases such as *Booker*, are highly persuasive to legislators and other policymakers. For example, *Booker* emphasized that sentences must be "reasonable,"[4] rejecting the idea that a statute, no matter how well crafted, can replace the well-informed discretion of a sentencing judge. In this respect, *Booker* can be seen as a continuation of the sentencing reforms of recent decades.

With an increased focus on the policy of sentencing, a review of the traditional theories of sentencing is in order. Sentencing has traditionally been defined by two inputs: the seriousness of the offense and the characteristics of the offender. The seriousness of the offense is both qualitative (typically a requisite mental state) and quantitative (financial loss, number of victims, and other factors). The key question asked in this line of thinking is how we measure the harm caused by the illegal act.

---

[3] United States v. Booker, 543 U.S. 220 (2005).

[4] *Id.* at 262-64.

The second input is the characteristics of the offender: his or her criminal record, culpability, willingness to accept responsibility (by plea bargain or during the sentencing phase), and so forth. The key question asked in this line of thinking is whether the defendant's conduct aggravated the offense or mitigated it. Rationales of punishment include deterrence, incapacitation, rehabilitation, retribution, "just deserts," and restorative justice.

II. HOW CYBER CRIMES ARE DIFFERENT

When addressing the nexus between sentencing and cyber crime, a fundamental question is: what is cyber crime? Most conferences on cyber crime focus on the offenders: who commits these kinds of crimes and how they commit them. Moreover, most training is devoted to how to detect cyber crime, apprehend the cyber criminals, and then prosecute them. Very little attention has been given to post-conviction matters, such as sentencing, victim impact, or alternative resolution. In preparing for the conference, it was very difficult to find people who were experts in both sentencing and cyber crime. I believe this touches upon an important shortcoming in our cyber crime jurisprudence: we have not yet adequately considered whether the traditional models of sentencing "fit" with cyber crime.

Cyber crime is both similar to and different from traditional crime. In many respects, traditional crimes have simply taken different forms by "migrating" to the Internet. For example, an e-mail fraud is quite similar to a traditional fraud. Scholars have debated whether cyber crimes are truly new and different crimes or just "old wine in new bottles."[5] Certainly, from the perspective of law enforcement, the crimes are often very similar—we apprehend the criminals, analyze the evidence forensically, and present that evidence at trial much the same way regardless of the type of crime. The tools and techniques for commission, detection, apprehension, evidence analysis, and presentation methods have all adapted to the evolution of technology and the Information Age.

---

[5] Joseph F. Savage, Jr., & Christina N. Smith, *New Wine in Old Bottles: Searching for a Rational Approach to Sentencing for New Economy Crimes*, 8 BUS. CRIME BULL. No. 6, at 1 (2001).

However, cyber crime is also different in many ways. It is often very difficult to detect, which presents new challenges for prosecution. It can also involve more complex potential for secondary and continuing victimization, even after perpetrators may be behind bars, such as when images of child pornography are distributed long after the abuse, or when a virus continues to replicate or is altered and re-released. Cyber crime is also less often a crime of passion, rage, or economic desperation, and more often a crime of defiance, overcoming a challenge, technological opportunism, or simple curiosity. The psychological motivations of cyber offenders are substantially different from those of traditional criminals. One scholar has also recently suggested that generativity is a key difference between cyber crime and traditional crime.[6]

During the first two days of this conference, a number of thought-provoking comments led me to think that perhaps it is in the aspect of victimization where cyber crime is most distinguishable from traditional crime. Cyber crimes can have a much more widespread impact upon a much larger number of victims per offense. They also present new and difficult issues regarding vulnerability of Internet users. Furthermore, prosecution of these crimes is more problematic because of the practical challenges of securing victims who can be available to testify, as well as the jurisdictional issues presented by interstate and international conduct. Finally, cyber crime often lacks a clearly identifiable victim, or worse, involves conduct from which victims are unable, in contrast to "traditional" crimes, to confront or "put a face on" the perpetrators. Law enforcement has traditionally been able to put a face on specific victims and perpetrators of criminal acts, but this is frequently not true with Internet crimes.

---

[6] Note, *Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442 (2006), *available at* http://www.harvardlawreview.org/issues/119/june06/note/immunizing_the_internet.pdf.

III. SHOULD SENTENCING LAW AND POLICY TAKE INTO ACCOUNT THE DIFFERENCES BETWEEN TRADITIONAL CRIMES AND CYBER CRIMES?

These considerations cause me to ask: can or should our old rules and policies regarding sentencing and punishment apply? When we talk about investigating cyber crime, we frequently assert that constitutional rules of criminal procedure pertaining to traditional crime apply in the same manner to cyber crime, only with some nuances. But what about our sentencing purposes and procedures and our societal purposes of punishment? Those fundamental concepts for responding to criminal conduct may well be radically different with regard to cyber crime. For example, if a cyber criminal is not motivated by forces the same as or similar to those motivating a regular criminal, our traditional models aimed at deterrence might not work well, or not work at all. Likewise, when the fact or scope of Internet victimization is undiscovered or difficult to detect until long after the event, our traditional models of measuring harm might fail to adequately address the problem.

In the courses I teach on sentencing, most of the material and discussion focuses on traditional crimes. When we consider the so-called "traveler" cases involving attempted sexual exploitation of children and the varieties of Internet fraud, for example, I have to wonder to what extent we are hitting the mark with sentencing. Does the digital and Internet age challenge or require us to re-examine our notions of case disposition and punishment? What should we do differently? If our goals may be different with regard to cyber criminals, what should our primary sentencing goals be? Do we seek to impose punishment that approximately equals the harm done, or do we focus on deterrence? Do we seek to rehabilitate offenders, or should we focus on protecting the public through incapacitation? Should our sentencing practices and concerns focus more on the offender or on the harm caused to victims?

On the concluding day of the conference, through the three presentations that follow, we begin to explore these issues more fully, as well as consider what is "reasonable," effective, and the best use of scarce law enforcement resources in sentencing and mitigating cyber crime. There are more questions in this area than can be addressed here, but the conference marks the beginning of a dialogue. Although there has been a significant amount of scholarly work on sentencing and cyber crime, few scholars have expertise in both subjects. In my view, the conference provides (outside of sentencing commission deliberations) one of the first ever explorations of the special issues arising from the intersection of sentencing and cyber crime. In short, what *can* we do and what *should* we do with cyber criminals after apprehension and adjudication, and why?

INTERNET CRIME VICTIMIZATION: SENTENCING

John F. Curran[*]

I. INTRODUCTION

As a former federal prosecutor who now works as a consultant specializing in computer forensic investigations, I regularly advise corporations and individuals in the aftermath of cyber-crime incidents. Generally, these persons are the victims of fraud or have had their computer networks hacked and their confidential (personal or business) information stolen. All too often, I respond to reports that employees are using the company's computer network to engage in a wide variety of criminal conduct such as fraud, viewing or sharing child pornography or engaging in the harassment of others. This conduct is merely illustrative of the types of activity falling within the ambit of cyber-crime.

The victims of cyber-crime require assistance on many levels. In the performance of an initial assessment, the priority for the investigator and the victim is to determine if the crime is continuing. If it is, the target of the attack or activity must be protected. With the compromise of corporate networks, one must identify and secure all network security gaps, including hidden "back doors" the intruder left behind to get back into the network in the case of just such a discovery. Another critical phase of the investigation is the determination of the full extent of the compromise to assess the potential data loss and harm caused. This step is particularly important for corporate networks containing personal identifying information of employees and/or consumers, such as social security numbers or credit card information, as most states require prompt notification to the persons whose information may have been compromised.[1] Throughout an incident response, one must preserve evidence in a forensically sound method for use in the identification and later prosecution of the offender.

---

[*] John Curran is Managing Director and Deputy General Counsel of Stroz Friedberg, LLC, a computer forensics and investigations firm. Mr. Curran previously served as a federal prosecutor and deputy general counsel for National Security Affairs at the F.B.I.

This article provides an overview of the role of the victim in the final stage of a cyber-crime investigation—after the criminal activity has been contained and the offender has been identified and prosecuted—namely, the punishment or sentencing phase.

Although many associate the sentencing phase of a criminal case with the offender, the victim can and should play a significant role in the proceeding that establishes the penalties imposed on a cyber-offender and the amount of compensation ordered to be paid to the victims for their losses.

Under federal statutes and applicable regulations, a cyber-crime victim, like all crime victims, has the right not only to attend all public proceedings associated with the offense, but can also actively participate in the sentencing hearing in some circumstances by providing oral and written statement to the court.[2] Additionally, the harm suffered by the victim is a critical element that a court must consider when determining the length of sentence to impose. Finally, at sentencing, the court is obligated by statute to order the defendant to provide full compensation to all identified victims for their actual losses caused by the offense.[3]

---

[1] For an overview of data breach notification obligations, see Eric Friedberg and Michael McGowan, *Lost Back-up Tapes, Stolen Laptops & Other Tales of Data Breach Woe,* COMPUTER & INTERNET LAW, Oct. 2006, at 6.

[2] *See* FED. R. CRIM. P. 32(i)(4)(B) (court must address a victim of a crime of violence or sexual abuse and afford an opportunity to speak). *See also* 18 U.S.C. § 3771 (Supp. IV 2004).

[3] 18 U.S.C. § 3663 (2000).

II. INTERNET CRIME VICTIM—JUSTICE FOR ALL

As a function of the modern focus on crime drama and reality television, when considering "rights" in the criminal realm, most people think first about the rights of the accused—the right to remain silent, the right to a trial, and the right to be represented by an attorney of choice. However, there is another protected class of persons in the criminal law—the crime victim. Although a victim's rights are not articulated in the United States Constitution, they are found throughout the United States Criminal Code.[4]

There is no more important statute confirming the vital place of victims in the criminal process than the Justice for All Act[5] (the "Act"). Signed into law on October 30, 2004, the Act defines a "crime victim" as "a person directly and proximately harmed as a result of the commission of a Federal offense."[6] The Act also recognizes the right of a crime victim to reasonable notification of and participation in all public court proceedings related the crime, including sentencing. The Act further recognizes the victim's right to "full and timely restitution."[7] Most significantly, the Act grants crime victims stand-

---

[4] Victim's bill of rights is often made a part of state constitutions.

[5] 18 U.S.C. § 3771.

[6] *Id.* § 3771(e). The definition of "victim" includes a corporate or other legal entity as well as natural persons. *See* 1 U.S.C. §1.

[7] Section 3771(a) recognizes the following rights for all crime victims:

> (1) The right to be reasonably protected from the accused.
> (2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused.
> (3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.
> (4) The right to be reasonably heard at any public proceeding in the district court involving release, plea sentencing, or any parole proceeding.
> (5) The reasonable right to confer with the attorney for the Government in the case.
> (6) The right to full and timely restitution as provided in law.
> (7) The right to proceedings free from unreasonable delay.
> (8) The right to be treated with fairness and with respect for the

ing to enforce these rights in federal court with an avenue of immediate appeal if dissatisfied.[8] The remedies for a violation of the Act include re-opening a plea or sentencing hearing, but do not extend to the right to obtain a new trial.[9] The accused is explicitly barred from any relief or remedy under the statute.[10]

The Act also directs the Attorney General to promulgate regulations to ensure compliance by Department of Justice officials.[11] The regulations require training related to the rights of victims and disciplinary sanctions, including termination, for employees who willfully fail to respect the rights of victims.[12]

Disregarding this growing wealth of authority protecting and indeed soliciting the participation of a victim in the prosecution and sentencing, one federal court granted a substantial sentencing reduction to a defendant based upon its finding that victim actively participated too much in the prosecution. However, this sentencing decision was reversed in *United States v. Yang*,[13] which held that a victim's participation in proceedings was not relevant to an offender's guilt or punishment.

---

victim's dignity and privacy.

Similarly, § 3510 explicitly orders the court not to exclude a victim of an offense from attending the trial. *See* 18 U.S.C. § 3510.

[8] *See e.g.*, Kenna v. United States Dist. Court for Cent. Dist. of Cal., 435 F.3d 1011 (9th Cir. 2006) (right to be heard at sentencing).

[9] *See* 18 U.S.C. § 3771(d)(5).

[10] 18 U.S.C. § 3771(d)(1).

[11] *Id.* § 3771(f)(1).

[12] *Id.* § 3771(f)(2). Pursuant to the Act's direction in May 2005, the Department of Justice promulgated and amended "Attorney General Guidelines for Victim and Witness Assistance," which implemented the new provisions, including providing for an administrative complaint process for aggrieved victims, *available at* http://www.usdoj.gov/olp/final.pdf [hereinafter *Guidelines*]. Indeed, the AG Guidelines are broader than the Act in extending a victim's rights to pre-prosecution stages, including the investigation of criminal activity. *Id.* at 22-26.

[13] 281 F.3d 534 (6th Cir. 2002).

III. Victim's Impact on Sentencing

Under federal sentencing statutes and guidelines, the harm or loss to the victim is often the single most significant factor a court uses to calculate the sentence under the United States Sentencing Guidelines. A brief primer on the interplay of the statutes, guidelines and discretionary decisions of the prosecutor and judge in the federal sentencing system follows.

A. Federal Criminal Code

Under federal law, a prosecutor's charging decision directly impacts the ultimate sentence imposed since the particular federal statutes violated by cyber-crime set the maximum and minimum sentence that can be imposed if there is a conviction. Although imbued with significant discretion in determining what charge to present to a grand jury, federal prosecutors are generally required to seek charges supported by readily provable facts that will generate the most serious sentence.[14] In making this charging decision, the Attorney General Victim Guidelines direct a prosecutor to seek a charge that ensures full restitution for victims.[15]

There are overlapping federal statutes potentially applicable to a cyber-crime incident. A single scheme or set of facts often form the basis for the violation of multiple federal criminal statutes. Take for instance an extortionate scheme where the cyber-criminal demands that a business pay thousands of dollars or it will be the target of a distributed denial of service attack[16] or the public disclosure of compromised business or computer security information. In such a case, the culprit may have violated the federal statute against extortion, called the Hobbs Act,[17] the Computer Fraud and Abuse Act (CFAA),[18] and possibly the wire fraud statute.[19] Similarly, a scheme to steal personal identifying information may violate the statutes related to identity theft,[20] access device (credit card) fraud,[21] bank fraud,[22] wire fraud and the CFAA.

---

[14] *See, e.g.*, Memorandum of Attorney General to Federal Prosecutors (Sept. 22, 2003).

[15] *Guidelines*, *supra* note 12, at 38-39.

[16] A DDoS is an attack on a network through flooding that network with communications and "thereby preventing legitimate network traffic." *See* http://www.cert.org/tech_tips/denial_of_service.html.

[17] 18 U.S.C. § 1951 (interference with commerce by threats or violence). Sec-

The sentencing scheme under each statute, however, is different. For example, the CFAA, which prohibits unauthorized intrusions to computers to commit, *inter alia*, fraud or cause damage provides for a maximum sentence of five years in many cases if the loss or damage is $5,000 or more, inclusive of a victim's costs in responding to the offense.[23] There is no minimum sentence. Other statutes may provide for enhanced penalties. For example, in most instances, the wire fraud statute and Hobbs Act provide for a twenty year maximum sentence.[24]

---

tion 1951 makes it a federal crime for a person who "in any way or degree obstructs, delays, or affects commerce . . . by robbery or extortion." 18 U.S.C. § 1951. In 2003, a twenty-nine year-old Kazakhstan citizen was sentenced to fifty-one months in prison following his conviction for unauthorized access to the computer system of Bloomberg LP and threatening to publicize the gaps in the system if not paid $200,000. *See* United States v. Zezev, No. 00 CR 01026 (S.D.N.Y. July 14, 2003).

[18] 18 U.S.C. § 1030. *See* discussion *infra* note 23. In 2006, a nineteen year-old, who launched distributed denial of service attacks (DDoS) from a "bot" net to disable the websites of his competitors, was sentenced to thirty months in prison and ordered to pay over $500,000 in restitution to the victims. *See* United States v. Arabo, No. 3:06-cr-00298-FLW (D.N.J. Aug. 25, 2006), *available at* https://ecf.njd.uscourts.gov (last visisted January 29, 2007).

[19] 18 U.S.C. § 1343. The wire fraud statute criminalizes the use of the wires in connection with a "scheme or artifice to defraud" or "from obtaining money by means of false or fraudulent pretenses."

[20] 18 U.S.C. § 1028. Aggravated identity theft, which punishes the use of stolen identity in the commission of another felony requires a consecutive two year sentence of imprisonment. *See* 18 U.S.C. § 1028A.

[21] 18 U.S.C. § 1029.

[22] 18 U.S.C. § 1344.

[23] *See* 18 U.S.C. § 1030(c)(2)(B). To reach the $5,000 threshold, the statute specifically defines "loss" to include "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at § 1030(e)(11).

[24] *See* 18 U.S.C. §§ 1951(a), 1343. Another critical statute for cyber crime investigators is the Controlling the Assault of Non-Solicited Pornography and

B. Sentencing Guidelines

Similar to the broad discretion of a federal prosecutor in the charging decision, federal judges had virtually unfettered authority to impose any sentence within the statutory range, which for certain violations could be a range of twenty to thirty years. To eliminate the widespread view that these sentencing disparities were inexplicable beyond the random assignment of a harsh or lenient sentencing judge, Congress enacted the Sentencing Reform Act of 1984,[25] creating the United States Sentencing Commission.[26] In 1987, the Sentencing Commission promulgated the Sentencing Guidelines mandating specified sentencing ranges for particular offenses with enhancements or reductions based upon factors called offense characteristics, including the extent of physical or financial harm to the victim and other adjustments such as a defendant's prompt acceptance of responsibility,[27] which establish the sentencing level at one of forty three levels on one axis of a grid. The other axis places numerical values on the defendant's prior criminal record. The intersection of the total offense level and criminal history produces the guideline sentencing range, within which the court had to sentence the defendant in most cases.[28]

For approximately twenty years, a federal court's discretion to depart from the guidelines range, either to increase or decrease a sentence was narrowly restricted to exceptional circumstances.[29] Under this sentencing scheme, the Court's function in sentencing was to determine any relevant and disputed facts at a sentencing hearing by a standard of prepon-

---

Marketing (CAN SPAM Act), 18 U.S.C. § 1037, which outlaws deceptive marketing and e-mail practices and provides for a maximum sentence of 3 years.

[25] *See* 28 U.S.C. §§ 991-98.

[26] 28 U.S.C. § 991.

[27] *See* U.S. SENTENCING GUIDELINES MANUAL § 3E1.1 (2005).

[28] *Id.*

[29] *See* U.S. SENTENCING GUIDELINES MANUAL § 5K2.0 (policy statement) permits a departure if "there exists an aggravating or mitigating circumstance . . . of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission." *Id.*

derance of the evidence and then mechanically apply the guidelines, which provided the range of months or years within which the ultimate sentence had to fall.

This mandatory scheme changed with *United States v. Booker*,[30] in which a majority of the Supreme Court, in an opinion authored by Justice Stevens, declared that the mandatory sentencing enhancements of the Guidelines based upon judicial fact finding was a violation of an accused's Sixth Amendment right to a jury trial. The court held: "Any fact . . . which is necessary to support a sentence exceeding the maximum authorized by facts established by a plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt."[31]

However, this decision did not sound the death knell for the Sentencing Guidelines. A different majority of the *Booker* Court, in an opinion written by Justice Breyer, rescued the Sentencing Guidelines by fashioning a remedy that retained the overall scheme but struck the mandatory application of the guidelines.[32]

Under current application, despite *Booker*, a sentencing proceeding has not changed much. The sentencing guidelines must be used by the federal courts to calculate a sentencing range and that range is afforded substantial weight. However, the court can vary from that sentence if that variance is reasonable after considering all of the factors of 3553(a).[33]

C. Imposing Sentence

Pursuant to 18 U.S.C. § 3553(a), the Court is directed to consider several factors when imposing sentence, only one of which makes specific reference to the victim, including:

---

[30] 543 U.S. 220 (2005).

[31] 543 U.S. at 244.

[32] *See* 543 U.S. at 245-46 (Breyer, J., second majority opinion).

[33] *See, e.g.*, United States v. Mashek, 406 F.3d 1012, 1017 (8th Cir. 2005); United States v. Lincoln, 413 F.3d 716, 717 (8th Cir.), *cert. denied*, 126 S.Ct. 840 (2005). Sentences are reviewed on appeal for reasonableness. *See* United States v. Fernandez, 443 F.3d 19 (2d Cir. 2006).

> (1) the nature and circumstances of the offense and the history and characteristics of defendant;
> (2) the need for the sentence imposed –
> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> (B) to afford adequate deterrence to criminal conduct;
> (C) to protect the public from further crimes of the defendant; and
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner
> . . .
> (7) the need to provide restitution to any victims of the offense.[34]

Despite only a single reference, the victim nevertheless plays a significant role in a court's determination of the seriousness of the offense and thereby establishing a just punishment for the offense. Moreover, although no longer mandatory, the Sentencing Guidelines provide a consistent metric by which to measure the seriousness of the offense and the impact on the victim.

D. The Sentencing Guidelines

Many financial cyber-crimes fall within a single guideline provision § 2B1.1, which governs sentencing proceedings for most property crimes, including fraud, theft and property destruction.[35] Section 2B1.1(a) establishes a base offense level which is increased based upon the single most important victim-related factor directly impacting the sentence, namely, the amount of loss. The Guidelines provide for incremental increases of the offense level where the loss exceeds $5,000 all the way up to losses of $400 million. These incremental increases can have the effect of raising the sentencing level anywhere from two up to thirty levels.[36] This loss calculation has a significant impact on the sentencing range. An offense involving less than $5,000 (assuming no other enhancements) could be as little as six months and the court could impose a probationary sentence under the guidelines. With a thirty level increase, the sentencing range could be as high as 188 to 235 months or almost twenty years.

---

[34] *See* 18 U.S.C. § 3553(a) (2000).

[35] Sentences for other cyber-crime violations, such as extortion or criminal infringement, are governed by different guidelines provisions, but incorporate the loss provisions of § 2B1.1. *See* U.S. SENTENCING GUIDELINES MANUAL §§ 2B3.3, 2B5.3(b)(1). Aggravated identity theft, see 18 U.S.C. § 1028A, requires a two-year sentence imposed consecutively to any other term of imprisonment.

Under the guidelines, the loss is defined as the actual or intended pecuniary harm caused to the victims of the offense charged and other losses related to the criminal conviction.[37] As referred to above, potential losses are to be considered even if the loss did not in fact occur and was impossible or unlikely to occur.[38] The court need not fix the amount of loss with certainty and can base its finding on a "reasonable estimate of the loss."[39] In addition, if loss cannot be reasonably determined, the court can use the offender's gain as an alternative measure. Significantly, losses caused by a violation of the CFAA include a victim's reasonable costs to respond to the offense.[40]

---

[36] *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(1).

[37] *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1, cmt. n.3. In addition, Guideline § 1B1.3 requires that the court consider not just the offense of conviction in establishing loss but also certain "relevant conduct," including "all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant; all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity, and all acts and omissions . . . that were part of the same course of conduct or common scheme or plan as the offense of conviction." U.S. SENTENCING GUIDELINES MANUAL § 1B1.3.

[38] *See Id.* § 2B.1. cmt. n.3(A)(ii). For an interesting view that the current federal sentencing scheme focused on economic crimes disproportionately punishes a class of cyber-criminals who, according to the author, provide benefits to the security of the Internet and prevents a more catastrophic attack, see Note, *Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442 (2006).

[39] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1, cmt. n.3(a).

[40] Loss includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, restoring the data, program, system, or information to its condition prior to the offense, and any lost revenue because of interrupted service." 18 U.S.C. §1030(e)(11) (2006). *See* U.S.

There are however some limits to what can be included in loss calculations. For example, pecuniary harm does not include emotional harm or harm to reputation. Interest is not included in the loss calculation.

Section 2B1.1 also provides an additional basis for an increase in the offense level if the offense involved ten or more victims of the offense.[41]

The Guidelines also provide for certain sentencing increases or "adjustments" including "Victim-Related Adjustments." These upward adjustments apply to hate crime offenses or where the offender knew or should have known that the victim was unusually vulnerable.[42]

E. Restitution

Victims of Internet crime can suffer substantial costs from the criminal activity and the response thereto, including investigation and restoring one's credit and computer network to health. We have seen how such costs directly impact the sentence imposed on the defendant. But, as a part of the sentence, the court can order the offender to compensate the victim. Indeed, according to a view expressed by the Department of Justice, the potential for obtaining restitution is one of the primary reasons given to persuade computer intrusion victims to report the crime to law enforcement.[43]

Under the Mandatory Victims Restitution Act of 1996 (MVRA), a defendant must make restitution to all identifiable victim or victims who have suffered a physical injury or pecuniary loss as the result of a federal offense.[44] Using virtually

---

SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n. 3(A)(III).

[41] *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)((2).

[42] *See* U.S. SENTENCING GUIDELINES MANUAL § 3A1.1. Additional adjustments, among others, apply to terrorism crimes or if the victim was a government official. *See id.* §§ 3A1.4, 3A1.2.

[43] *See* Richard P. Salgado, Working with Victims of Computer Network Hacks, 49 United States Attorneys' USA Bulletin 2, at 4 (Mar. 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/ usamarch2001_6.htm (last visited Jan. 24, 2007).

[44] *See* 18 U.S.C. § 3663A(2) (2000).

identical language as used to define a crime victim in the Justice for All Act, the MRVA requires restitutions for victims "directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered."[45]

There is an exception to the requirement for restitution, where the court finds the number of victims is so large that making restitution is impracticable or if the court finds that determining complex issues of fact related to the amount of victims' losses would unduly complicate or prolong the sentencing process.[46] It is submitted that this exception should only be used in the most extraordinary circumstances where there are identifiable victims of a defendant's conduct. In fact, the Justice for All Act makes clear that the court should "fashion a reasonable procedure" to ensure to protection of victims rights, including restitution.[47]

Distinct from Guidelines "loss" calculation, restitution amounts are based solely on the actual loss suffered by the victim, including lost income and other expenses "incurred during participation in the investigation and prosecution of the offense."[48] The Probation Department is instructed to obtain statements of loss from all victims identified by the prosecutor and investigative agency. This information is included in the pre-sentence report furnished to the court and the parties prior to sentence. The burden to prove these restitution amounts falls on the prosecutor, and the court determines factual disputes concerning restitution by the preponderance of the evidence.[49] Indeed, the court has the authority to set a date not later than ninety days following sentencing for a "final determination of the victim's losses."[50]

---

[45] *Id.*

[46] 18 U.S.C. § 3663A(c)(3).

[47] 18 U.S.C. § 3771(d)(2).

[48] 18 U.S.C. § 3663A(b)(4). Recently, in its Summary of Interim Recommendations, the President's Identity Theft Task Force recommended that Congress amend §§ 3663(b) and 3663A(b) to explicitly allow compensation for the time spent by consumers in remediation of their credit and avoiding additional harm. *See* President's Identity Theft Task Force, Summary of Interim Recommendations, at 6, http://www.ftc.gov/os/2006/09/060916interimrecommend.pdf (last visited Jan. 25, 2007).

[49] 18 U.S.C. § 3664(e).

A final aspect of sentencing with particular relevance of the protection of victims is the authority of the court to impose restrictive conditions of release as a part of a sentence of probation or during the period of supervised release, which is a mandated term of supervision following incarceration for most federal offenses. This authority may have significant relevance for victims of Internet crime, where there is a high degree of recidivism.[51] These conditions of release must be reasonably related to the sentencing factors of § 3553(e), discussed above, such as deterrence and protection of the public, and can include restrictions on the type of employment and can even limit or deny access to computers.

IV. CONCLUSION

A cyber-crime victim plays important and varying roles in the prosecution and sentencing of the offender. They are witnesses to the state's prosecution and they are in a real sense parties in interest to that case. Beyond the assistance that a victim may need to respond and remediate the damage done, the victim may be unfamiliar with their rights under the law and will need the assistance of prosecutors and other victim/witness professionals to ensure that their rights are protected.

---

[50] 18 U.S.C. § 3664(d)(5).

[51] *See* Christopher M.E. Painter, *Supervised Release and Probation Restrictions in Hacker Cases,* 49 United States Attorneys' USA Bulletin 2, at 1 (March 2001), available at http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm (last visited Jan. 24, 2007).

THINKING THROUGH SENTENCING IN COMPUTER HACKING CASES: DID THE U.S. SENTENCING COMMISSION GET IT RIGHT?

Richard W. Downing[*]

The factors courts consider in sentencing traditional criminal violations often do not include all of the appropriate factors that courts should consider in sentencing computer hackers. In particular, certain relevant factors cannot readily be quantified in monetary terms, such as invasions of privacy and risks to critical economic infrastructures. This article discusses the relevant considerations for sentencing in computer hacking cases and evaluates the effectiveness of the 2003 reforms to the U.S. Sentencing Guidelines.

Over the past five years, the prevalence of computer hacking crimes and the significance of their consequences have continued to grow. The conviction of Scott Levine in 2005 marked a milestone in the theft of electronic information: by accessing corporate databases of an Arkansas company without authorization, he and his conspirators copied over one *billion* records containing personal information.[1] Similarly, the MS Blaster worm caused a new level of economic disruption when it shut down railroad switching computers across the Southeastern United States.[2] The serious harm caused by these attacks on computers and information[3] clearly show the need for the justice system to adequately deter and punish this conduct.

---

[*] Richard Downing received a B.A. in Political Science from Yale University and a J.D. from Stanford Law School. He is currently Assistant Deputy Chief of the Computer Crime and Intellectual Property Section, United States Department of Justice. The views expressed in this article are those of the author and do not necessarily reflect the positions or opinions of the United States Department of Justice.

[1] *Marketer Found Guilty Of Data Theft,* WASH. POST, Aug. 13, 2005, at D2; Press Release, U.S. Dep't of Justice, Former Officer Of Internet Company Sentenced in Case of Massive Data Theft from Acxiom Corporation (Feb. 22, 2006), http://www.cybercrime.gov/levineSent.htm.

When considering the need for deterrence, it is important to understand the difficulty of successfully catching and punishing hacking offenders. This difficulty arises from a number of factors. First, the victims of computer hacking often do not detect the unauthorized access on their systems, and organizations that do detect hacking often do not report it to law enforcement because of fears of adverse publicity.[4] Second, once law enforcement opens an investigation, the crime is very hard to investigate. The protocols underlying the Internet were not designed with identification of users as a priority,[5] and criminals can achieve anonymity fairly easily through the use of throw-away email accounts and proxy servers that hide the true source of communications.[6] Third, the high cost of training and equipping law enforcement officers to investigate computer hacking means that for the foreseeable future, there will not be adequate investigative capability. This problem is particularly severe for smaller police agencies in state and local jurisdictions, and for many foreign law enforcement agencies. Thus, the likelihood of punishment for any particular offense remains quite low.

---

[2] Jonathan Adams & Fred Guterl, *Bringing Down the Internet*, NEWSWEEK, Oct. 28, 2003, *available at* http://msnbc.msn.com/id/3339638/; *'Slammer' Worm Could Pick Up Steam Monday*, CNN.com, Jan. 27, 2003, http://www.cnn.com/2003/TECH/internet/01/26/internet.attack/; Press Release, U.S. Dep't of Justice, Louisiana Man Arrested for Releasing 911 Worm to WebTV Users (Feb. 19, 2004), http://www.cybercrime.gov/jeansonneArrest.htm.

[3] Although the definition of what constitutes "cybercrime" is far from settled, *see* Richard W. Downing, *Shoring up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Laws to Combat Cybercrime,* 43 COLUM. J. TRANSNAT'L L. 705, 711 (2005), this article will consider those crimes in which the "victim" of the crime is a computer or information stored by a computer. Thus, unauthorized access to a computer, damage to a computer, or threats to damage a computer all fall within this rubric. The United States Code focuses these offenses in title 18, section 1030, although other parts of title 18 contain related offenses. *See, e.g.*, 18 U.S.C. § 2701 (2000) (criminalizing access to or malicious destruction of email). This article will not consider traditional crimes facilitated by computers and the Internet, such as online fraud and the electronic distribution of child pornography.

[4] *See* Computer Security Institute & Federal Bureau of Investigation, 2006 CSI/FBI Computer Crime and Security Survey, July 13, 2006, at XX, http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml.

[5] Hearing on the Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age Before the Senate Committee on the Judiciary, 106th Cong. (Sept. 6, 2000) (statement of Vinton G. Cerf).

[6] Michael E. O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9

Under one theory of sentencing, the level of deterrence caused by the criminal justice system is the likelihood of apprehension and punishment multiplied by the degree of punishment.[7] In other words, in a world of rational actors with perfect information, as the likelihood of apprehension drops, the level of punishment must increase in order to obtain the same level of deterrence for a particular crime. According to this theory, given the relatively low likelihood of apprehension for cybercrimes, the criminal justice system needs to assure appropriately stiff sentences in order to achieve more effective deterrence.[8]

Commentators, of course, have pointed out that those intent on violating the law do not always act rationally, nor do they necessarily have accurate information about the likelihood of their apprehension and eventual punishment.[9] Nevertheless, cybercrimes by their very nature allow offenders to commit the offenses without leaving their homes and with a veil of anonymity. This lack of contact with the victims of their crimes and insulation from law enforcement may cause them to be

---

GEO. MASON L. REV. 237, 261 (2000).

[7] Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968); Cesare Beccaria, *On Crimes and Punishments*, *in* ON CRIMES AND PUNISHMENTS AND OTHER WRITINGS 1, 21 (Richard Bellamy ed. & Richard Davies et al. trans., 1995).

[8] *See* O'Neill, *supra* note 6, at 259-64.

[9] *See* Lucian Ayre Bebchuk & Luis Kaplow, *Optimal Sanctions When Individuals Are Imperfectly Informed About the Probability of Apprehension*, 21 J. LEGAL STUD. 365 (1992); Micheal K. Block & Robert C. Lind, *An Economic Analysis of Crimes Punishable by Imprisonment*, 4 J. LEGAL STUD. 479 (1975). One commentator has suggested, however, that computer criminals may be more rational than other criminals in evaluating the costs and benefits of committing a crime because the Internet provides a low-cost way for potential criminals to learn about the law and its sanctions. O'Neill, *supra* note 6, at 268.

under-deterred. Only successful prosecution and significant punishments will supply prospective cyber-criminals with the information needed to create real deterrence.

Congress has recognized the importance of providing tough penalties for network attacks. In 2001 and again in 2002, Congress raised the maximum penalties for certain portions of the Computer Fraud and Abuse Act.[10] In addition, Congress instructed the U.S. Sentencing Commission to reconsider how the U.S. Sentencing Guidelines (hereafter, "USSG") treat computer hacking offenses. This review resulted in revisions in 2003 that improved the way in which the USSG treat such offenses. Yet flaws in these revisions, as well as advances in the technology and the manner in which the offenses are committed, suggest that the USSG need a fresh look.[11]

This article explores the various factors that courts should take into consideration when sentencing computer hacking offenses. Many of the considerations that would normally apply to white collar crime offenses are appropriate here as well. But because many additional harms occur—especially those that cannot readily be measured in monetary terms—courts should consider a variety of other factors to avoid inappropriately light sentences. For example, courts must take into account physical harm to individuals, privacy invasions, and the impact on critical economic infrastructures and governmental functions. Only a broad-based consideration of the effects of such crimes will allow for appropriate sentencing, and the Sentencing Commission should revise the USSG to take these factors into account.

---

[10] Both the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (hereinafter "USA PATRIOT Act"), and the Homeland Security Act, Pub. L. No. 107-296 (2002) (hereinafter "Homeland Security Act"), raised the maximum penalty for computer hacking offenses. For example, the USA PATRIOT Act increased the maximum penalty for intentionally damaging a computer from five years imprisonment to ten years. USA PATRIOT Act, § 814. The Homeland Security Act addressed the situation where such offenses cause bodily harm. Under the revised title 18, section 1030(c)(5), a court has the discretion to impose life in prison where death results from intentional damage to a protected computer. Homeland Security Act, § 225(g). Indeed, as recently as 2006, the House Judiciary Committee approved a bill that would again raise the maximum penalties for computer hacking offenses. H.R. 5318, 109th Cong., 2nd Sess., § 8 (2006), *available at* http://thomas.loc.gov.

[11] In 2005, the Supreme Court struck down mandatory application of the USSG. United States v. Booker, 543 U.S. 220 (2005). Despite this ruling, the USSG remain an important guide for sentencing, and courts have continued to apply them in most cases. The Sentencing Commission recently reported that in fiscal year 2006, courts imposed sentences outside of the guidelines only 14.1% of the time (excluding downward departures at the request of the government). United States Sentencing Commission, Special Post-Booker Coding Project, July 6, 2006, at 1, *available at* http://www.ussc.gov/Blakely/PostBooker_060106.pdf. Because *Booker* has given federal courts greater discretion, they can apply the factors discussed in this article without waiting for the U.S. Sentencing Commission to amend the USSG.

MONETARY HARM

Courts have historically looked at the monetary harm suffered by a crime victim when considering the seriousness of a particular offense, particularly where the crime has a financial motivation. For example, when considering the appropriate punishment for insurance fraud or embezzlement, the financial harm to the victim provides a rough approximation of the significance of the offense, and sentencing schemes such as the USSG direct judges to increase the penalty in proportion to the financial harm.[12]

This theory of sentencing applies equally to hacking crimes, but with some slight adaptations. Certainly, some hacking crimes are completely analogous to traditional white collar crimes. If a hacker breaks into the online banking servers of a financial institution and transfers money into an account he controls, courts should give appropriate weight to the financial harm suffered by the victim just as they would in a real-world bank fraud case.

Damage to Computers or Information

Where the goal of the crime is simply to cause damage to the victim computer, however, the economic losses incurred by the victim are certainly relevant but must be evaluated with care. In the case of computer hacking, "damage" does not, of course, usually mean the physical destruction of a tangible thing. Instead, it means an impairment to "the integrity or availability" of data or a computer system.[13] This type of damage can be accomplished, for example, by deleting data, by changing information in a database, by crashing a computer, or by simply making it unavailable to users by flooding its network connection with junk information. Very often, this sort of "damage" does not cause any permanent harm to the victim computer. Once the problem is corrected—the computer is repaired or the flood of junk information cut off—the computer can continue to operate as it did prior to the crime. Yet the cost of these repairs can be significant, particularly where the owner needs to hire an outside computer security consultant.[14] Thus, sentencing courts should consider these costs in calculating the economic harm caused by the offense.

---

[12] United States Sentencing Guidelines, § 2B1.1(b) [hereinafter U.S.S.G.].

Moreover, in some cases the sole goal of the hacking crime is to make a computer unavailable. In one case, the owner of an online satellite television company paid hackers to use a "denial of service attack" to shut down his competitor's computers for two weeks. When the victim company could not sell its services, it lost profits.[15] In sentencing the offender, a court should take into account this real financial harm.

In addition, some hacking crimes create significant costs in restoring the owner's confidence in the integrity of data. If a hacker intrudes into the servers that handle a hospital's billing, for example, the system administrators may not be able quickly to determine what records the hacker changed. It may take many employees many days to reconstruct the data in order to make sure that they have detected all of the alterations. Courts should consider the cost of restoring the computer owner's confidence in the data stored on the victim computer when evaluating the significance of the hacker's crime.

---

[13] *See, e.g.*, 18 U.S.C. § 1030(e)(8).

[14] *See, e.g.,* Press Release, U.S. Dep't of Justice, British National Charged with Hacking Into N.J. Naval Weapons Station Computers, Disabling Network After Sept. 11; Indictment Also Filed in Virginia for Other Military Instructions (Nov. 18, 2002), *available at* http://www.cybercrime.gov/mckinnonIndict2.htm ($900,000 loss); Press Release, U.S. Dep't of Justice, Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced to 41 Months for Unleashing $10 Million Computer "Time Bomb" (Feb. 26, 2002), *available at* http://www.cybercrime.gov/lloydSent.htm ($10,000,000 loss); Press Release, U.S. Dep't of Justice, Plano Man Convicted of Computer Sabatoge (Nov. 21, 2005), *available at* http://www.cybercrime.gov/kwongConvict.htm ($600,000 loss).

[15] Matt Viser, *Sudbury Man Hunted by FBI for Cybercrime*, BOSTON GLOBE, Dec. 12, 2004, at 1. Saad Echouafni was indicted in Los Angeles for this crime but has not been arrested. For the FBI wanted person notice, see http://www.fbi.gov/wanted/fugitives/cyber/echouafni_s.htm. *See also* David Ashenfelter, *Southfield Man, 19, Pleads Guilty in Web Hacking Case*, DETROIT FREE PRESS, Apr. 13, 2006, available at http://www.freep.com/apps/plcs.d1l/article?AID=20060413/NEWS03/604130507/1001/NEWS.

Theft of Information

A slightly different situation occurs, however, where the hacking crime involves the "theft" of information. In general, the value of real-world stolen property is a good measure of the significance of the crime.[16] The theft of electronic information, however, differs in one significant respect: the offender generally only *copies* the data and does not deprive the owner of possession or use of it. While this circumstance will reduce the harm experienced by the victim, the value of the information remains a good proxy for the significance of the offense. By comparison, consider the situation in which a bank detects embezzlement quickly and stops the transfer of funds out of the victim's account. Like the owner of illegally copied data, the bank account owner is not deprived of the use of his property, but no one would argue that the amount of money in the attempted transfer is irrelevant at sentencing.

Moreover, in the case of computer data, it may prove difficult at times to establish the value of the information. Some types of information, such as a customer list, have a market value that can be established at trial through expert testimony or by introducing evidence that the offender sold it to another person.[17] But it may be impossible to put a price tag on other types of information, even though it plainly cost someone a considerable amount of money to create the data. For example, an individual broke into a NASA computer in 1999 and stole a software program developed to control the physical environment on the International Space Station.[18] It cost NASA $1.7 million dollars to develop this software, but it probably has no value on the open market.[19] Similarly, in 2000 several employees of Lucent Technologies stole the source code to a new server designed to handle voice and electronic data that cost millions of dollars to develop.[20] The offenders intended to transfer the technology to China.[21] Because of business decisions, however, Lucent discontinued its product, and the current market value of the software may be zero.[22] In these situations, the cost of developing the information provides a reasonable alternative measure of its value, and courts should utilize this value in calculating the harm caused by the offense.

---

[16] *See* 18 U.S.C. § 2314 (creating federal violation for interstate transportation of stolen goods only where stolen goods' value exceeds $5,000); U.S.S.G., § 2B1.1(b) (2004) (recommended sentence for theft and embezzlement offenses increases in proportion to the loss sustained by the victim). Congress has also used this criterion in setting the maximum penalty for hacking crimes where the offender obtains information from a computer without authorization. 18 U.S.C. § 1030(c)(2)(B)(iii) (where the value of information obtained exceeds $5,000, maximum penalty increases from one year in prison to five years in prison).

Sentencing Guidelines

Amendments to the USSG in 2003 greatly improved the treatment of damage to a computer. Under Section 2B1.1, the USSG define "actual loss" to include the following harms, regardless of whether they were reasonably foreseeable:

---

[17] Of course, the price at which stolen data is sold, sometimes called "black market" price, generally substantially under represents the true value of the information. Buyers of stolen data presumably would not pay full price because of the risk that the data may not be reliable or genuine, and because they risk prosecution for possession of the stolen information.

[18] David Stout, *Youth Sentenced in Government Hacking Case*, N.Y. TIMES, Sept. 23, 2000, at A9; Press Release, U.S. Dep't of Justice, Juvenile Computer Hacker Sentenced to Six Months in Detention Facility (Sept. 21, 2000), *available at* http://www.cybercrime.gov/comrade.htm.

[19] Press Release, *supra* note 18.

[20] Craig S. Smith, *Chinese Tread Warily in Secrets-Theft Case,* N.Y. TIMES, May 8, 2001, at C6; Press Release, U.S. Dep't of Justice, Lucent Scientists Arrested, Charged with Stealing Tech Secrets for Joint Venture with China-controlled Company (May 3, 2001), *available at* http://www.cybercrime.gov/ComTriadarrest.htm.

[21] Press Release, *supra* note 20.

[22] *Id.*

> Any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.[23]

This broad definition, now identical to the statutory definition of "loss" in 18 U.S.C. § 1030(e) provides good coverage for the kinds of economic harms victims experience when their computers are shut down or where offenders impair their data or system security.

This loss definition, however, completely ignores the harm to victims caused by the theft of information. Indeed, by providing a specific definition of loss for offenses under 18 U.S.C. § 1030, it makes it harder for the government to argue that courts should take into account other measures of loss—such as the market value of information—and to counter defendants' arguments that a court should ignore the value of illegally copied information because the offense did not interfere with the victim's use of the information. Thus, the U.S. Sentencing Commission should consider broadening the treatment of loss to cover information theft offenses. Moreover, the USSG should explicitly direct judges to take into account the development cost of information as an alternative to the other measures of the value of information, such as market value.

The following language would accomplish this result:

> (III) *Offenses Under 18 U.S.C. § 1030.*—In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages

---

[23] U.S.S.G. § 2B1.1, n.3(A)(v)(III) (2004).

incurred because of interruption of service.[24]

In addition, where the offense involves obtaining information, actual loss includes the value of that information, regardless of whether the owner was deprived of its use. If the market value of information is difficult or impossible to determine or does not adequately reflect the significance of the information, the value of the information will be the cost incurred to develop or compile the information.

THE INTENT OF THE OFFENDER

As with many traditional crimes, sentencing courts should consider a computer crime offender's intent. Where the object of the crime is the theft of information,[25] fraud,[26] or extortion,[27] the definition of the offense already includes a particular mental state. Offenders, of course, seldom *recklessly* extort someone or *negligently* obtain money under false pretenses. Courts should have little difficulty in taking their criminal intent into account.

In the case of damage to a computer, however, the actor could have a variety of mental states. In some cases, the offender has acted intentionally to access a computer without authorization but then inadvertently causes the system to crash. This negligent or reckless damage can have serious consequences—such as when a juvenile shut down the regional airport in Worcester, Massachusetts, in 1996 by breaking into a telephone company computer and accidentally causing the machine to crash[28]—but the offender should be treated more leniently than if the conduct were fully intentional. By contrast, Jeffery Lee Parson released a worm that not only spread aggressively and monopolized communications bandwidth, but it caused computers around the world to deluge Microsoft with spurious data that shut down its Internet connection for hours.[29] Plainly, courts should treat these two offenders differently due to their differing degrees of intent, quite apart from the damage that their acts actually cause.

---

[24] 18 U.S.C. § 1030(e)(11).

[25] *See, e.g.*, 18 U.S.C. § 1030(a)(2).

[26] *See, e.g.*, 18 U.S.C. § 1030(a)(4).

[27] *See, e.g.*, 18 U.S.C. § 1030(a)(7).

[28] Press Release, U.S. Dep't of Justice, Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport: First Federal Charges Brought Against a Juvenile for Computer Crime (Mar. 18, 1998), *available at* http://www.cybercrime.gov/juvenilepld.htm.

Sentencing Guidelines

Congress created a graduated sentencing scheme for the Computer Fraud and Abuse Act. Unauthorized access to a computer when combined with any amount of damage constitutes a one-year misdemeanor offense,[30] but that offense rises to a five-year felony where the offender causes the damage *recklessly*.[31] The statute reserves the ten-year maximum imprisonment for offenders who damage computers *intentionally*.[32]

Like the statutory maximums created by Congress, the USSG explicitly address the question of intent. If the offender causes damage intentionally, the USSG call for a four-level increase.[33] Unfortunately, the subsection that contains this increase contains a number of bases for an increased guideline range, and this mix of factors does not always lead to the appropriate outcome. The source of this problem is the subsection's directive to "Apply the Greatest" of three elements, each of which should be treated separately in most cases. For example, the first of these elements directs the court to increase a defendant's guideline range by two levels if the offense includes the unauthorized access to a military computer or the theft of personal information. If the offender also intentionally causes damage, however, he triggers the second element, a four-level increase, and the court will ignore the first element. Thus, if the offender intentionally damages a computer that controls the power grid, the USSG would assign him the exact same guideline range as someone who intentionally damages a grocery store computer. This outcome makes little sense, and the Sentencing Commission should allow each of these elements to apply independently of one another.

---

[29] Mike Carter & Kim Peterson, *Man Caught by Own Worm: 'Blaster' Variant's Author Foiled by his Cyberprints*, SEATTLE TIMES, Aug. 30, 2003, at A1; Press Release, U.S. Dep't of Justice, Minneapolis, Minnesota 18 year old Arrested for Developing and Releasing B Variant of Blaster Computer Worm (Aug. 29, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/parsonArrest.htm.

[30] 18 U.S.C. § 1030(c).

[31] *Id.*

[32] *Id.*

[33] U.S.S.G. § 2B1.1(14)(A)(ii).

The following wording would accomplish this result:

> (14)(A) (Apply the greatest) If the defendant was convicted of an offense under 18 U.S.C. § 1030 and:
>
> (i) the offense involved a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security increase by TWO levels.
>
> (ii) the offense caused a substantial disruption of a critical infrastructure, increase by SIX levels. If this level is less than level TWENTY-FOUR, increase to level TWENTY-FOUR.
>
> (B) If the defendant was convicted of an offense
>
> (i) under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, increase by TWO levels.
>
> (ii) under 18 U.S.C. § 1030(a)(5)(A)(i), increase by FOUR levels.

SMALL HARMS TO MANY VICTIMS

In many cases, computer hacking crimes cause harm to thousands or even millions of victims. In many such cases, however, the harm sustained by each individual computer owner may be comparatively slight and difficult to assess. For example, a home user's computer could become infected by a computer worm that causes the operating system to crash unexpectedly. The computer user may need to spend several hours finding, downloading, and using a software tool to clean up the system, and she might lose data from a document that was open at the time of the computer crash. Likewise, a worm could copy all address books on the victim computer and send the information out to the worm's author for later use in sending spam. In both these cases, the victim does not suffer any significant financial loss or easily measurable harm. Yet when these small inconveniences or invasions of privacy of thousands of users are added together, the total harm caused by the crime can be considerable.

This common scenario can cause difficulties in the context of a criminal prosecution, however. Prosecutors may find it difficult to present evidence of these small harms at the sentencing phase of a trial. As the government plainly cannot present the testimony of thousands of witnesses or even identify every single person who has suffered harm, courts should allow the government to present the testimony of several representative victims. The government may then be able to call an expert witness to extrapolate from these examples based on the expert's knowledge of the effects of the computer worm. In this way, courts can gain at least a rough assessment of the crime's aggregate harm in many cases.

Sentencing Guidelines

The USSG contain an effective approach to address those situations where calculations of the total harm are uncertain or impossible. In addition to increasing the guidelines' range based on harms measured in monetary terms, the USSG direct courts to increase sentences where the crime affects multiple victims.[34] Section 2B1.1(2) raises the guidelines' range by two levels where the crime involves more than ten victims, by four levels where it involves more than fifty victims, and by six levels where it involves more than 250 victims.[35] This supplemental increase helps to assure an appropriate outcome where many victims receive a small financial harm.

---

[34] U.S.S.G. § 2B1.1(2).

[35] *Id.* Of course, virtually every crime involving a virus, worm, or botnet will have more than 250 victims, so one could conceive of a special category for these offenses with extremely widespread effects. However, the six-level increase for more than 250 victims probably adequately addresses the need for increased sentences for these offenses.

Unfortunately, the USSG do not similarly take into account victims who do not suffer financial harm. Application Note 1 restricts the definition of "victim" to include only those who have suffered loss that can be measured in monetary terms.[36] Thus, if the worm invades the privacy of many computer owners but does not cause any quantifiable monetary loss, the increases for multiple victims do not apply. Yet it makes no sense for the guidelines to direct courts to enhance sentences for privacy invasions but then define "victim" to be only those that suffer monetary harm. The Sentencing Commission should address this problem by amending the definition of "victim" so that it includes persons whose privacy was invaded by the criminal offense.

INVASIONS OF PRIVACY

As computers have become increasingly ubiquitous in our society, the amount of personal information stored in digital format continues to multiply. Companies store vast amounts of sensitive information about people, such as medical and financial records. Individuals have also taken advantage of computer resources, storing information such as diaries, personal correspondence, online banking and investing, wills, tax returns, and calendars. As more and more computer networks serve as repositories for private information, computer intrusions now have unprecedented potential to expose the personal information of hundreds or thousands of users at once.

Computer intruders attempt to obtain such information for a wide variety of reasons. For example, in 2000, a group of hackers broke into computers across the United States as part of a scheme to steal credit cards and other identity information and use it to commit fraud. Vasiliy Gorshkov was convicted, among other things, of possessing over 50,000 credit card numbers.[37] Hackers have also accessed medical records for financial gain. Several years ago, a hacker accessed a Pittsburgh hospital to obtain the medical records of a popular country western singer in order to later sell them to a tabloid newspaper.[38] Many information thefts, however, are motivated by curiosity or a prurient interest, rather than a monetary one. Prosecutors recently indicted five people for designing and selling a software program that buyers could use to spy on others, such as their spouses, girlfriends, or ex-lovers. Once surreptitiously installed on a computer, the "Loverspy" program would access stored files and relay them to person who installed it. Many others across the country have been indicted for using "Loverspy."[39]

---

[36] U.S.S.G. § 2B1.1, n.1.

[37] Press Release, U.S. Dep't of Justice, Russian Computer Hacker Sentenced to Three Years in Prison (Oct. 4, 2002), *available at* http://www.cybercrime.gov/

Courts may find it difficult to evaluate and properly sentence this sort of conduct. As discussed above, when an intruder copies digital information, it generally does not prevent the owner from continuing to use that information, and it may be difficult to measure the privacy invasion in monetary terms. In addition, even where the crime has an economic motivation—such as where a hacker steals financial information and uses it to commit fraud—the crime generally causes a significant privacy invasion quite apart from the monetary harm. Indeed, where a bank makes the customer whole, the privacy invasion may be the most salient harm. Moreover, in most cases, if the person who steals the information discloses that information to someone else, the privacy invasion is aggravated. Thus, where a hacker sells identity information on the black market,[40] or where a spurned lover intercepts private emails and then posts them on the Internet, the severity of the

---

gorshkovSent.htm.

[38] *Selling Singer's Files Gets Man 6 Months*, HOUSTON CHRONICLE, Dec. 2, 2000, at A2.

[39] *Alleged Spyware Mastermind, Buyers of the Program Indicted*, LOS ANGELES TIMES, Aug. 27, 2005, at B4; Press Release, Dep't of Justice, Creator and Four Users of Loverspy Spyware Program Indicted (Aug. 26, 2005), *available at* http://www.cybercrime.gov/perezIndict.htm.

[40] *See, e.g.*, Press Release, Dep't of Justice, Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy — Shadowcrew Organization Was Called 'One-Stop Online Marketplace For Identity Theft' (Nov. 17, 2005), *available at* http://www.cybercrime.gov/mantovaniPlea.htm.

harm increases dramatically.

Sentencing Guidelines

Policymakers considering the drafting of guidelines to address privacy invasions are faced with a difficult task. Plainly, not all information is equally sensitive, and creating rules to take into account varying sensitivities between different types of "private" information can prove elusive. For example, no one expects publicly listed phone numbers to remain private, but if hackers get access to a celebrity's address book the invasion of privacy can be significant.[41] Similarly, a home user's computer may contain thousands of family photographs that the owner does not regard as particularly confidential, but that person would almost certainly feel quite differently if a pedophile were to gain access to pictures of his or her children.

Moreover, individuals have differing sensitivities to the disclosure of their information. Some people may care little about the disclosure of their wills or tax returns, while others would be deeply disturbed to have this information made public. Indeed, some people have a deep-seated concern about the disclosure of even the more mundane aspects of their lives—such as where they choose to shop or how much money they spend on telephone calls.

For this reason, sentencing guidelines should allow a large degree of discretion to the sentencing court to examine the facts of a particular case, evaluate the harm to the particular victims, and fashion an appropriate sentence. Such guidelines can, however, play a role in assuring that sentencing courts do not ignore the various ways in which privacy can be invaded.

The USSG does a credible job of meeting these two goals. On the one hand, the USSG prescribe a two-level increase where the offense involves the intent to obtain "personal information."[42] The definition of "personal information" provides courts with the following non-exclusive list:

---

[41] *Paris' Pals Besieged with Calls After Her Cell Phone is Hacked*, CHICAGO SUN TIMES, Feb. 23, 2005, at 52 (hackers gained access to celebrity Paris Hilton's cell phone and posted phone numbers from the phone on the Internet).

[42] U.S.S.G. § 2B1.1(14)(A)(i)(II).

> Personal information' means sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including e-mail; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.[43]

Notably, this definition does not require that the personal information be in the possession of the person about whom the information pertains.

On the other hand, the USSG provide broad discretion for courts to increase the penalty where the facts of a particular case demonstrate a "substantial" privacy invasion. They explicitly recommend an upward departure from the guideline range that would otherwise apply where "[t]he offense caused or risked substantial non-monetary harm. For example, the offense . . . resulted in a substantial invasion of a privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records)."[44]

Thus, for example, where a man obtains unauthorized access to the personal emails of a woman as part of a stalking offense, the USSG would call for a two-level increase for the obtaining of personal information and encourage the court to increase the sentence above the guideline range due to the significant privacy invasion.

The USSG do have one shortcoming: they do not explicitly address the situation in which private information is disclosed beyond the individual who gains unauthorized access to it. Because this act virtually always increases the significance of the privacy invasion, the Sentencing Commission should consider amending the USSG to include an additional two-level increase for such an action.

Building on the changes proposed above, the following amendment would accomplish this result:

---

[43] U.S.S.G. § 2B1.1, n.13(A).

[44] U.S.S.G. § 2B1.1, n.19(A)(ii).

> (B) If the defendant was convicted of an offense
> (i) under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, increase by TWO levels. If the offense involved the disclosure of such personal information to another, increase by an additional TWO levels.

PHYSICAL HARM TO INDIVIDUALS

Although there has been no documented case of a death caused by unauthorized access to a computer, a number of close-calls suggest that it is only a matter of time. For example, in 1997, one hacker recklessly damaged a telecommunications switch that interrupted service at a regional airport in Massachusetts. For hours, approaching pilots were unable to activate the runway landing lights, and communications with emergency services were inoperable.[45] A similar risk to life and limb occurred when Rajib Mitra disrupted police radio service in Madison, Wisconsin, on Halloween, 2003. Although no physical injuries were reported, it was in part the threat of such harm that caused the judge to sentence Mitra to eight years in prison.[46] It is also not difficult to imagine a malicious hacker disrupting service at a hospital with the intent of causing harm to patients.

Of course, courts routinely sentence for offenses that involve physical injury and death. Courts can readily take into account the conduct if they examine the offender's mental state *with respect to the physical injury*. For example, if the offender fully *intends* to access a hospital computer and alter a patient database, but is *reckless* about the possibility that death would result, then the appropriate penalty should emulate that for reckless homicide. Similarly, if the hacker manipulated a patient's hospital records with the intent to cause that person to die, then the penalty should be commensurate with first degree murder.

---

[45] Press Release, U.S. Dep't of Justice, Juvenile Computer Hacker Cuts off FAA Tower at Regional Airport—First Federal Charges Brought Against a Juvenile for Computer Crime (Mar. 18, 1998), *available at* http://www.cybercrime.gov/juvenilepld.htm.

[46] Reid J. Epstein, *Hacker Convicted in Police Radio Case—He'll Be Sentenced May 12 for Transmitting Sexually Explicit Sounds*, MILWAUKEE JOURNAL SENTINEL, Mar. 5, 2004, at B1; Kevin Murphy, *8-Year Sentence for Radio Interference—UW Grad's Actions Labeled Terrorism*, CAPITAL TIMES, May 13, 2004, at 1B.

Sentencing Guidelines

The USSG section that relates to hacking offenses, Section 2B1.1, covers a broad range of white collar crimes. As such, death or physical injury rarely results from these offenses, and the section does not address this possibility with much precision. In particular, § 2B1.1(12) requires a mere two-level increase "[i]f the offense involved . . . the conscious or reckless risk of death or serious bodily injury."[47] Section 2B1.1 has no explicit increase where injury or death actually occurs, however. Instead, the USSG give courts broad discretion to issue sentences above the guideline range where, "for example, in an 18 U.S.C. § 1030 offense involving damage to a protected computer, if, as a result of that offense, death resulted."[48]

This broad discretion seems out of place compared with the precision with which the USSG treats injury and death in other sections. For example, § 2A1.1 through 2A1.4 creates a sensible structure for the various mental states related to homicide, and there is no reason that § 2B1.1 could not directly cross-reference that section. Indeed, this type of cross-reference is used in other parts of the USSG, such as § 2L1.1 (Smuggling, Transporting, or Harboring an Unlawful Alien). Such a cross-reference could also clarify that in applying § 2A1.1-4, courts should assess the offender's mental state with respect to the death itself. Similarly, § 2B1.1 should be amended to include explicit treatment of offenses that cause physical injury. Section 2L1.1 again provides a suitable model: a two-level increase for offenses that cause bodily injury, a four-level increase for serious bodily injury, and a 6-level increase for

---

[47] U.S.S.G. § 2B1.1(12). This section also provides that if the resulting guideline range is below 14, to raise it to 14, thus assuring a recommended sentence of at least 15 months.

[48] U.S.S.G. § 2B1.1, n.19(a)(ii).

"permanent or life-threatening bodily injury."[49] These amendments would provide courts with appropriate direction and harmonize this section with other similar USSG sections.

HARM TO CRITICAL INFRASTRUCTURES

"Critical infrastructures" have been defined as "systems and assets vital to national defense . . . economic security, public health or safety."[50] Such infrastructures include the distribution of electricity, banking and finance, telecommunications, government emergency services, and the water supply. Moreover, in the United States, operation of these infrastructures increasingly relies on computer networks, and much attention has been focused on assuring the continuity of these systems.[51] This attention seems appropriate—a catastrophic failure of the electrical grid in the Northeastern United States and Canada, caused by the accidental failure of a single computer, knocked out power to fifty million people, many of whom lost power for more than a week.[52]

Computer crimes have resulted in severe threats to critical infrastructures, such as when hackers gained unauthorized access to computers that controlled the flows of gas in the distribution pipelines of Gazprom, the largest natural gas company in the world. Russian officials reported that no ill effects occurred.[53] Similarly, in 1998 a hacker reportedly broke into the computer system that runs Arizona's Roosevelt Dam, attaining complete command of the system controlling its massive floodgates. If the sixty-five billion cubic feet of water restrained by the dam had been released, the consequences could have been disastrous for Mesa and Tempe, Arizona, two communities on the flood plain below the dam with a combined population totaling nearly one million people.[54]

---

[49] U.S.S.G. § 2L1.1(b)(6).

[50] *See, e.g.,* U.S.S.G. § 2B1.1, n.13(a).

[51] *See, e.g.,* National Strategy to Secure Cyberspace, Feb. 2003, *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[52] *The Blackout of 2003: The Overview*, NEW YORK TIMES, Aug. 15, 2003.

[53] Paul Quinn-Judge, TIME EUROPE, *Cracks in the System—Russia's Cybercrime Squad Fears the Next al-Qaeda Attack May Be on Crucial Computer Networks*, June 17, 2002, at 31, *available at* http://www.time.com/time/europe/magazine/article/0,13005,901020617-260664,00.html.

Moreover, some cybercrimes have actually caused harm to critical infrastructures. For example, in addition to damaging computers around the world and slowing communications networks, the *blaster worm* shut down the computers that controlled rail switching in the Southeastern United States, disrupting schedules or forcing trains to move very slowly. More ominously, it also crippled the safety system of a nuclear power plant. Luckily, the nuclear reactor was offline for maintenance at the time, and no harm occurred.[55] Plainly, courts will have to consider how to appropriately sentence offenders who threaten or disrupt critical infrastructures.

Some of these types of attacks might cause losses that can be measured in monetary terms, and experts could testify at sentencing hearings about them. For example, if a computer attack shuts down the New York Stock Exchange for two days, it would be possible at least to calculate the profit lost by the stock exchange itself and the expenses required to repair the system. Other loss calculations may be impossible, however. How would one measure in dollar terms the interruption of the water supply or the disruption of government emergency services? Courts will need to find ways to take into account these other non-monetary harms.

Drafting guidelines to take non-monetary harms into account, however, is not easy. Because of the significant possibility of inadvertent harm, for example, it makes sense to increase the penalty for any crime that results in unauthorized access to a computer used to control a critical infrastructure regardless of whether harm results. But in order to apply this increase, should prosecutors have to prove that the offender knew the nature of the victim computer? A good argument can be made that these computers require such stringent protection that the offender should receive higher punishment regardless of intent. In other words, offenders take the risk when they break into another's computers and the burden should be on them to know on whose computer they are trespassing.

---

[54] Barton Gellman, *Experts Fear Cyber-attack by Al Qaeda — Computers' Role in Controlling Infrastructure, Combined with Security Gaps and Terrorists' Skills, Prompts Concerns About a Catastrophe*, CHICAGO TRIBUNE, July 4, 2002, at 9. U.S.S.G. § 2B1.1, Application Note 19(b). It is worth noting that application Note 19(b), unlike the definition of "critical infrastructure" itself, refers only to "national" economic security and "national" public safety. This change in wording suggests that the Commission intended that courts impose the 6-point increase where the harm to critical infrastructures is local or regional and impose sentences above the standard guidelines range where the harm to the economy or public safety is of national significance.

[55] Frank James, *Teen Held in Net Attack, But Bigger Fears Remain,* CHICAGO TRIBUNE, Aug. 30, 2003, at 1.

Another significant problem in developing guidelines is how to take into account the fact that not all "critical infrastructure computers" have the same significance. For example, every computer that routes traffic on the Internet supports the "telecommunications infrastructure." Yet many of these computers go offline periodically, and disruption of a single computer will not have any noticeable impact on communications traffic. Sentencing guidelines must have some mechanism for courts to differentiate between the intentional disruption of a minor router and an attack that interrupts the flow of oil in the Alaskan pipeline.

Finally, some harms to critical infrastructures threaten life and limb. Those that create this threat—or that actually cause physical injury or death—should be treated with appropriate severity.

Sentencing Guidelines

The U.S. Sentencing Commission has made a number of important changes to the USSG to take into account computer crimes involving critical infrastructures. For example, the USSG supply a good definition of "critical infrastructure":

> "Critical infrastructure" means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems,

> financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public.[56]

In addition, the USSG instruct judges to take into account the significance of the harm to the infrastructure itself. If the crime in any way involves a computer used to "maintain or operate" a critical infrastructure, the USSG call for a two-level increase.[57] If the offense causes a "substantial disruption" to a critical infrastructure, however, the increase jumps to six levels, with a minimum level of twenty-four.[58] Finally, if harm to the infrastructure is so substantial as to have a "debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters," the USSG recommend courts impose a sentence above the standard guidelines range.[59] Although a six-level increase for substantially disrupting a critical infrastructure may be slightly inadequate, the overall framework is very good.

The USSG does, however, have several flaws in its treatment of offenses that affect critical infrastructures. First, as identified above in Section II of this article, § 2B1.1(14) does not allow for cumulative increases where the crime involves intentional damage to a computer and the offense disrupts a critical infrastructure. This lack of aggregation means that the person who intentionally shuts down a state's power grid will get the same six-level increase as the person who accidentally does so. In addition, as noted above in Part V of this article, § 2B1.1 does not provide adequate cross references to the sections governing bodily injury and death.

---

[56] U.S.S.G. § 2B2.3, n.1.

[57] U.S.S.G. § 2B1.1(14)(A)(i).

[58] U.S.S.G. § 2B1.1(14)(A)(iii), (B).

[59] U.S.S.G. § 2B1.1, n.19(B). It is worth noting that Application Note 19(B), unlike the definition of "critical infrastructure" itself, refers only to "national" economic security and "national" public safety. This change in wording suggests that the Commission intended that courts impose sentences above the standard guidelines range only where the harm to the economy or public safety is of national significance.

HARM TO GOVERNMENT FUNCTIONS

Like attacks on critical infrastructures, computer intrusions involving certain government computers often cause harms that cannot be measured in monetary terms. For example, elections increasingly rely on computers, both for the casting and the tallying of votes. Disruption of a computer used to tally votes on an election day may be relatively inexpensive to repair, but it can have a significant impact on the perception of fairness among the voters. How can one place a value on the reliability of an election?

Similarly, computer networks are used in furtherance of the administration of justice—by state, local, and federal law enforcement agencies, by jail and prison agencies, by probation and parole offices, and by local, state and federal courts. Such networks play a role in ensuring that the justice system performs effectively and efficiently so that dangerous criminals are kept off the streets. In one notable case, a convicted felon hacked into the computer network in San Bernadino County, California, and changed the records to show that charges pending against him were dismissed.[60] If criminals can modify their sentences, gain early release, or disrupt the functioning of the courts, it could cause a grave impact on the public's faith in the fairness of the criminal justice system.

Moreover, attacks on military computers can cause harms far beyond those that can be measured by the cost of cleaning up a damaged computer network. For example, a computer intrusion that discloses troop and equipment locations could gravely harm national security and endanger soldiers on the battlefield. Because of the importance of such government functions and because it is generally impossible to measure these harms solely in terms of repair costs or lost profits, courts should give careful consideration to these factors in sentencing offenders.

---

[60] David Seaton, *Hacker Accesses Computer System for Riverside County, Calif., Superior Court*, THE PRESS-ENTERPRISE, (Riverside, CA), June 14, 2002, *available at* 2002 WLNR 9026366.

Sentencing Guidelines

The USSG provide for increased penalties for intrusions into some, but not all, government systems. Section 2B1.1(14)(A)(i) provides for a two-level increase for *any* intrusion into "a computer system . . . used by or for a government entity in furtherance of the administration of justice, national defense, or national security."[61] This provision appropriately reflects the gravity of such attacks: offenders should be strongly deterred from such conduct.

The USSG also do a credible job in addressing attacks on justice or national security computers that do in fact result in a disruption of service. Courts should rule that defense and criminal justice computers meet the general definition of "critical infrastructures" ("systems and assets vital to national defense, national security, economic security, public health or safety"[62]) making their disruption qualify for the sentencing provisions relating to critical infrastructures described above. Defense and criminal justice computers, however, are strangely absent from the definition's list of examples, and the Sentencing Commission should clarify this oversight.[63] As noted above, the USSG also direct courts to impose sentences in excess of the guidelines range when "the disruption to the critical infrastructure(s) is so substantial as to have a debilitating impact on national security, national economic security, national public health or safety."[64] This provision sensibly gives courts the discretion to fashion quite severe penalties in truly egregious cases.

---

[61] U.S.S.G. § 2B1.1(14)(A)(i).

[62] U.S.S.G. § 2B1.1, n.13(A).

[63] The following wording would accomplish this correction:

> Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations *such as the administration of justice and national security or* that provide essential services to the public.

CONCLUSION

As crimes and offenses continue to change with the advance of technology, courts will increasingly be called upon to fashion sentences for crimes that do not fit the traditional patterns. These crimes remain very difficult to investigate, making it likely that many offenses will go undiscovered and many offenders unpunished.[65] Where the likelihood of apprehension is low, it becomes all the more important that courts impose appropriately lengthy sentences in order to deter the criminal conduct.

These offenses, however, require consideration of a broad range of factors, some of which may be foreign to judges not familiar with information technology. Prosecutors therefore have the burden to educate courts about the real harms that these crimes cause through the testimony of victims and technology experts. The U.S. Sentencing Commission could ease this task and facilitate improved sentencing in computer crime cases by amending the USSG in the ways detailed in this article.

---

[64] U.S.S.G. § 2B1.1, n.19(B).

[65] *See* O'Neill, *supra* note 6, at 261.

CREATIVE SANCTIONS FOR ONLINE INVESTMENT FRAUD

Jayne W. Barnard[*]

As long as promoters have sought to raise money for their ventures, fraud has been a feature of the marketplace.[1] Throughout commercial history, some stock promoters have touted their product, misrepresented its value, and manipulated its pricing. Eager investors have often parted with their money impulsively, overpaid for worthless or near worthless stock, and later complained that they were misled.

This Article will examine the current environment in which stock promoters sell their wares. Increasingly, stock scams are not confined to face-to-face encounters or multi-telephone-line, high-testosterone "boiler rooms." Rather, investment fraud—like other forms of fraud—is migrating to the Internet. According to the National White Collar Crime Center, online investment fraud is now the fifth most common form of Internet fraud.[2] Since its creation in 1998, the SEC's Office of Internet Enforcement has handled cases involving hundreds of millions of dollars in investor losses.[3]

---

[*] James Goold Cutler Professor of Law, The College of William & Mary. Thanks to William & Mary students Melissa Cross '06, Brent Dougal '07, and Chris Toepp '07, who provided research support for this article. Thanks also to John Tucker and Wayne Logan for their helpful comments.

[1] The Roman playwright Plautus describes the "puffers" and the "impudent, talkative, and malevolent fellows" who populated the Roman Forum in the second century B.C. EDWARD CHANCELLOR, DEVIL TAKE THE HINDMOST: A HISTORY OF FINANCIAL SPECULATION 4 (2000).

[2] NAT'L WHITE COLLAR CRIME CTR. & FBI, IC3 2005 INTERNET CRIME REPORT Chart 5 (2005), *available at* http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf.

[3] *See, e.g.*, Andrew Leckey, *Fraud Dresses Up On Web, But It's Still Crime*, CHI. TRIB., Apr. 2, 2006 at C6 (noting that, since 1998, the office has handled

Part I of this Article will briefly examine the current patterns of securities fraud schemes, especially those schemes that depend on the use of the Internet (including e-mail) for successful execution.

Online investment fraud is usually the subject of civil enforcement, both at the state and federal level, not criminal prosecution. Still, some securities fraud schemes—and particularly some Internet-based securities fraud schemes—warrant criminal prosecution. Part II of this Article will explore the current tools available to sanction securities law violators. Under federal law, several sentence enhancements are available that seem particularly applicable to online investment schemes; state law, too, provides some guidance on the appropriate sentence for securities law violators.

Current federal law, however, has some holes in it as regards online fraud schemes, including online investment schemes. In Part III of this Article, I will sketch out three possible amendments to the Federal Sentencing Guidelines that would improve the sentencing regime available for perpetrators of online investment fraud. I will also encourage the creation of a securities fraud registry—modeled after sex offender registries—to assist potential investors in knowing with whom they are dealing.

I. TODAY'S ELECTRONIC INVESTMENT SCHEMES

Historically, many securities frauds involved face-to-face encounters in which an aggressive salesman promoted (or "touted") an overvalued security.[4] In the 1960s, so-called "boiler rooms" emerged, in which a battery of high-pressure salesmen worked from phone banks, making cold calls to customers' offices and homes and soliciting the purchase of securities—often thinly-traded stocks known as "penny stocks."[5]

---

nearly 600 Internet-related cases).

[4] *See, e.g.*, SEC v. N. Am. Fin. Co., Fed. Sec. L. Rep (CCH) ¶ 91,241 (Apr. 17, 1959) (describing sale of securities by members of a "sales organization" involving multiple misrepresentations and omissions).

[5] *See, e.g.*, In re Waldman & Co., 1967 SEC LEXIS 2603 (Jan. 30, 1967)

Today, more and more investors are seeking investment opportunities on the Internet. Their comfort level in doing so traces to four factors: (1) many of these investors experimented with day trading during the 1990s and became accustomed to the process of identifying and purchasing stocks online; (2) search technologies such as Google have made the search for investment opportunities cheap and easy; (3) issuer websites, investor message boards, and chat rooms have streamlined the process of gathering information about companies and their prospects—both reliable and unreliable information; and (4) payment systems such as PayPal and the routine use of credit cards online have made the entire process of buying securities as easy as buying a pair of shoes.

There is also a seductive aspect of searching for investment opportunities online. Somehow, a person who goes looking for investment information and comes up with something she thinks is an attractive opportunity feels more empowered and confident than had she received a cold call from a salesman. One assumes that a securities salesman has a strong interest in making a sale and may over-promote the product, but somehow visiting a website that facilitates a securities purchase seems more objective—and safer—than making a decision in response to an obvious solicitation. In fact, it often feels as if no solicitation has taken place at all but rather the investor has made her own, exciting discovery.

Investor message boards have played a special role in building investors' confidence in today's markets. Even though most investors presumably understand that message boards can be manipulated by posters harboring a hidden agenda, they still may attribute to bulletin board posts a sense of real-

---

(examining the practices of an early boiler room operation); SEC v. Wellshire Secs. Inc., Litigation Release No. 12411, 1990 SEC LEXIS 428 (Mar. 14, 1990) (describing a classic boiler room scheme in which the salesmen "made exorbitant and baseless price predictions" and sold securities that were unsuitable for their customers); SEC v. Wolfson, Litigation Release No. 18930, 2004 SEC LEXIS 2349 (Oct. 14, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (describing a penny stock boiler room operation located physically in Vientiane, Laos).

ity they would not attribute to a sales call. That is, reading dozens of posts about a company may reassure the reader that she has captured the insights of others with no axe to grind, confirm that others have made the same decision (to buy or sell) being contemplated by the reader, and persuade her that she has the benefit of some kind of insider information. As one experienced investor recently revealed in a memoir about the HealthSouth fraud case, "I was convinced that message boards provide valuable access to investment information available nowhere else."[6]

These developments—and investors' increasing comfort level with making investment decisions unaided and online—inevitably have fostered a growing online fraud industry.

What do these online stock frauds look like? Not surprisingly, they often look much like yesterday's fraud schemes, just slicker. Thus, we find issuers selling securities from corporate websites that misrepresent their assets, revenues, and realistic prospects for the future;[7] issuers purporting to sell securities then absconding with the proceeds of the offering;[8]

---

[6] WILLIAM CAST, M.D., GOING SOUTH: AN INSIDE LOOK AT CORRUPTION AND GREED, AND THE POWER OF THE HEALTHSOUTH MESSAGE BOARD 39 (2005). Investor message boards may also impart a special sense of community amongst participants. After repeated visits, message board visitors may develop a sense of trust in what they read, without considering where the information is really coming from. Constance Z. Wagner, *Securities Fraud in Cyberspace: Reaching the Outer Limits of the Federal Securities Laws*, 80 NEB. L. REV. 920, 944 (2001).

[7] *See, e.g.*, SEC v. Inv. Tech., Inc., Litigation Release No. 18970, 2004 SEC LEXIS 2624 (Nov. 15, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (describing promoter's claims that an Internet-based gambling site had already handled $4 million in wagers, when in fact the company had no history of operations or revenue); SEC v. Toks, Inc., Litigation Release No. 18309, 2003 SEC LEXIS 2040 (Aug. 25, 2003), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2003.shtml (describing issuer's claims it intended to launch tender offers for several major public companies, when in fact it had no revenue or assets and only one employee, so it "had no ability to conduct the contemplated tender offers").

[8] *See, e.g.*, SEC v. Richmond, Litigation Release No. 17609, 2002 SEC LEXIS 1773 (Jul. 12, 2002), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml (noting that much of the proceeds of an Internet-based Ponzi scheme had been deposited into the defendant's personal bank ac-

issuers selling unregistered securities from their websites;[9] issuers selling interests in "Ponzi schemes"[10] or "pyramid" schemes;[11] issuers promoting so-called "risk-free" investments when in fact the investments are risky or even fictitious;[12] and issuers engaged in a modern version of the "pump-and-dump" or stock price manipulation scheme.[13] Some of the schemes are surprisingly simple—"touting" violations, for example, where the promoter fails to disclose that he is being compensated for his role in the offering,[14] or where the issuer

---

counts).

[9] *See, e.g.*, SEC v. Phoenix Telecom, L.L.C., Litigation Release No. 18971, 2004 SEC LEXIS 2627 (Nov. 16, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (involving the sale and leaseback of pay telephones over the Internet, in a scheme that raised over $74 million); SEC v. Grabarnick, Litigation Release No. 18833, 2004 SEC LEXIS 1781 (Aug. 16, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (involving the sale of unregistered LLP units through bulk e-mail ("spam") and websites, in a scheme that raised over $10 million).

[10] *See, e.g.*, SEC v. Johnson, Litigation Release No. 19592, 2006 SEC LEXIS 535 (Mar. 7, 2006), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2006.shtml (describing Internet-based Ponzi scheme); SEC v. Par Three Fin., Inc., Litigation Release No. 19348, 2005 SEC LEXIS 2197 (Aug. 25, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (same); SEC v. Richmond, Litigation Release No. 17609, 2002 SEC LEXIS 1773 (July 12, 2002), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml (same).

[11] *See, e.g.*, SEC v. Int'l Heritage, Inc., Litigation Release No. 17832, 2002 SEC LEXIS 2845 (Nov. 8, 2002), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml (describing defendants' Internet-based pyramid scheme).

[12] *See, e.g.*, SEC v. Learn Waterhouse, Inc., Litigation Release No. 18959, 2004 SEC LEXIS 2579 (Nov. 4, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (describing a so-called "risk free" investment program that raised $24.5 million); SEC v. Nnebe, Litigation Release No. 18302, 2003 SEC LEXIS 2021 (Aug. 22, 2003), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2003.shtml (describing another "risk free" offering that raised $2 million from 118 investors).

[13] *See infra* notes 16-28 and accompanying text.

[14] *See, e.g.*, SEC v. Spradling, Litigation Release No. 19505, 2005 SEC LEXIS 3268 (Dec. 21, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (alleging failure to disclose the amount and nature of the promoter's compensation for the sale of penny stocks); In re Flynn, Exchange Act Release No. 7641 (Feb. 24, 1999), *available at* http://www.sec.gov/litigation/admin/adminarchive/adminarc1999.shtml (alleging nondisclosure of at least $183,200 in cash and 322,500 shares of stock for the promoter); In re

falsely claims that its products are FDA-approved.[15]

Some online stock frauds, however, depend on the unique features of the Internet for their success and represent more than just a high-tech version of age-old techniques. Here are some examples.

In one scheme that gained notoriety on the news program *60 Minutes*, a high school student named Jonathan Lebed engaged in a fairly simple pump-and-dump scheme using the Internet.[16] First he purchased large blocks of shares in thinly-traded microcap companies, using his father's trading account.[17] Then, using multiple identities and usernames, Lebed made thousands of posts onto Yahoo's investor message boards, offering statements like "[this stock is] about to take off," "[it will be] the next stock to gain 1000%," and "[this] is the most undervalued stock ever."[18] By creating the appearance of intense enthusiasm across a large number of investors, Lebed was able to sell his shares at the top of the market, and profited by at least $272,000.[19]

In another scheme, another high school student, Benjamin Snyder, held stock in Viragen International, Inc., and wanted to sell his stock at a profit.[20] He not only posted false statements on investor message boards, but also created a phony news story that looked like it had come from the Bloomberg news service.[21] He used the name of an actual Bloomberg re-

---

Hastings Commc'ns, Inc., Exchange Act Release No. 7643 (Feb. 24, 1999), *available at* http://www.sec.gov/litigation/admin/adminarchive/adminarc1999.shtml (alleging nondisclosures of compensation at stockprofiles.com).

[15] *See, e.g.*, SEC v. Vaso Active Pharm., Inc., Litigation Release No. 18834, 2004 SEC LEXIS 1784 (Aug. 17, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml.

[16] In re Lebed, Exchange Act Release No. 43307, 2000 SEC LEXIS 1964 (Sept. 20, 2000), *available at* http://www.sec.gov/litigation/admin/adminarchive/dminarc2000.shtml.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] In re Snyder, Litigation Release No. 46108, 2005 SEC LEXIS 1619 (June 25, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml.

[21] *Id.*

porter as the purported source of the news story.[22] People reading about Viragen on the message boards often clicked through to the phony Bloomberg news story, and were persuaded on that basis to buy—and drive up the price of—the stock.[23]

Yet a third Internet scheme involved law students at Georgetown Law School.[24] The students created a website—"Fast-Trades.com"—on which they offered stock recommendations.[25] They promoted their website by posting hundreds of messages on investor message boards.[26] "These messages disguised the authors' connection with the site and misrepresented the investment success they achieved from following Fast-Trades' recommendations."[27] The students relied on a growing subscriber base at Fast-Trades.com to buy stock on the basis of the website's recommendations, thus driving up the stock price, whereupon the students would sell their pre-purchased shares.[28] The students netted more than $345,000 on the scheme.

Other pump-and-dump schemes involved the creation of—and links to—phony "analysts' reports,"[29] the creation of a "Red Hot Stocks" website to promote the defendants' companies and their stocks,[30] and the distribution of "spam" e-mail messages endorsing the defendants' specified companies.[31]

---

[22] *Id.*

[23] *Id.*

[24] SEC v. Colt, Litigation Release No. 16461, 2000 SEC LEXIS 376 (Mar. 2, 2000), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2000.shtml.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] SEC v. MegaMania Interactive, Inc., Litigation Release No. 19369, 2005 SEC LEXIS 2315 (Sept. 9, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (involving the distribution of hundreds of thousands of unsolicited e-mails containing phony "analysts' reports" and recommendations that characterized MegaMania as "Our Most Aggressive Stock Buy Recommendation"); SEC v. Inv, Tech., Inc., Litigation Release No. 18970, 2004 SEC LEXIS 2624 (Nov. 15, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (involving the creation of press releases and "analysts' reports" that described the issuer, which had no history of operations or revenue, as "a leader" in the online gaming industry).

[30] SEC v. Franklin, Litigation Release No. 19466, 2005 SEC LEXIS 2952

Recently, some new forms of online investment frauds have emerged and these, too, are dependent on the special features of the Internet. In one scheme, the promoters created a "virtual stock exchange" on which—for a fee—people could trade in "virtual stock."[32] Through computer programming, the price of the virtual stock would rise and fall.[33] The promoters promised a minimum gain on each "virtual" investment of 10% per month (or 215% a year).[34] In fact, the scheme was an old-fashioned Ponzi scheme, in which later-arriving investors would fund the payoffs to earlier-arriving investors.[35] The scheme netted more than $5 million before it was interrupted by the SEC.[36]

Another scheme that depends on the Internet is the stock-related "cybersmear." Here, short-sellers drive down the price of a stock by posting negative, false information on investor message boards.[37]

Yet another Internet-dependent scheme is the recently-dismantled "auto-surfing" scheme.[38] Here, the promoter induced victims to participate in a program in which they were promised payment merely for "clicking and looking" at certain web pages.[39] The premise behind the scheme was that com-

---

(Nov. 16, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml.

[31] SEC v. Rice, Litigation Release No. 17732, 2002 SEC LEXIS 2364 (Sept. 17, 2002), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml.

[32] SEC v. SG Ltd., Litigation Release No. 18181, 2003 SEC LEXIS 1378 (June 9, 2003), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2003.shtml.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Byron D. Hittle, *An Uphill Battle: The Difficulty of Deterring and Detecting Perpetrators of Internet Stock Fraud*, 54 FED. COMM. L.J. 165, 170 (2001).

[38] SEC v. Johnson, Litigation Release No. 19592, 2006 SEC LEXIS 535 (Mar. 7, 2006), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2006.shtml.

[39] *Id.*

panies that advertise on the Internet are willing to pay to increase traffic to their web sites.[40] These companies hire an auto-surf firm or "host," which in turn pays individual web surfers to view certain web sites on an automatically rotating basis.[41] The more sites the individual visits, the more money he or she stands to earn.[42]

The problem with this scheme was that, once a victim was "hooked" with small payments for "clicking and looking," there was a charge to continue in the program.[43] Victims were asked to purchase "membership units," which would entitle them to additional "clicks" each day.[44] The scheme, however, was really a Ponzi scheme. Before being shut down, the website was ranked as the 352nd most heavily-trafficked web site in the United States.[45] The scheme is said to have raised more than $50 million from over 300,000 investors worldwide.[46]

Two final Internet-based securities fraud schemes do not, in fact, involve securities fraud at all, in any conventional sense. In the first case, the defendant hacked into an online trading account and electronically caused an unknown victim to "purchase" soon-to-be-worthless stock options owned by the defendant.[47] The defendant thereby avoided $37,000 in foreseeable losses.[48] Because the victim did not in fact make any investment decision, but was an unwitting buyer, this scheme does not seem to fit the traditional pattern of inducing a purchase based on a material misstatement or omission. The second case involved the giveaway of "free stock" in order to create the appearance of an active market, with recipients induced to sign up for the offer with gross overstatements of the "free" stock's value.[49] Here, too, the victims did not make investment decisions—they merely accepted gifts of (usually worthless) stock.[50]

---

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] SEC v. Dinh, Litation Release No. 18696, 2004 SEC LEXIS 939 (May 6, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml.

[48] *Id.*

II. THE EXISTING TOOLKIT

Since 1934, securities law violations have been subject to a civil enforcement regime presided over by the Securities and Exchange Commission (SEC). Over that period, the SEC has acquired a wide range of enforcement tools, which today includes the authority to seek a court-ordered asset freeze;[51] to enter and enforce its own cease-and-desist orders against wrongdoers;[52] to suspend or bar regulated professionals from continuing to serve in their professional roles;[53] to seek a "penny stock bar,"[54] an "officer and director bar,"[55] injunctive relief,[56] the imposition of civil penalties,[57] the appointment of a court-appointed receiver,[58] and disgorgement of profits to compensate victims.[59]

---

[49] *See* U.S. SEC. & EXCH. COMM'N, SEC BULL. NO. 99-83, SEC BRINGS FIRST ACTIONS TO HALT UNREGISTERED ONLINE OFFERINGS OF SO-CALLED "FREE STOCK," (July 22, 1999), *available at* www.sec.gov/news/headlines/webstock.htm.

[50] *Id.*

[51] *See, e.g.*, SEC v. Tanner, Litigation Release No. 19325, 2005 SEC LEXIS 1990 (Aug. 4, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (involving the interruption of the sale of so-called "high yield" bonds, in which the proceeds of the offering—more than $15 million—were sent offshore; the court entered an asset freeze against the issuer, individual defendants, and one defendant's mother).

[52] *See, e.g.*, SEC v.Vindman, Exchange Act Release No. 53654, 2006 SEC LEXIS 862 (Apr. 14, 2006), *available at* http://www.sec.gov/litigation/opinions/opinionarchive/opinarch2006.shtml (imposing a cease-and-desist order on promoter of a penny stock scheme).

[53] *See, e.g.*, SEC v. First Access Fin. L.L.C., Litigation Release No. 18984, 2004 SEC LEXIS 2715 (Nov. 23, 2004), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2004.shtml (barring the defendant from association with any broker or dealer, with the right to apply ro re-association after three years); SEC v. Ware, Exchange Act Release No. 51878, 2005 SEC LEXIS 1441 (June 20, 2005), *available at* http://www.sec.gov/litigation/aljdec/34-51878.htm (permanently disqualifying the defendant—an attorney—from appearing or practicing before the SEC).

[54] *See, e.g.*, SEC v. Ives Health Co., Litigation Release No. 19043, 2005 SEC LEXIS 128 (Jan. 21, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (barring the defendant from participating in any penny stock offering for three years).

[55] *See, e.g.*, SEC v. Saad, Litigation Release No. 19159, 2005 SEC LEXIS 711

This Article, however, is about what happens when the SEC cedes its authority to the Department of Justice to pursue criminal sanctions against a defendant. Specifically, this Article considers some of the ways in which federal prosecutors might deal with online investment frauds in the criminal context.

Under the Federal Sentencing Guidelines (Guidelines), prosecutors necessarily must deal with both the "offense level" of the crime (based upon the amount of loss occasioned by the

---

(Mar. 29, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (permanently barring the defendant from serving as an officer or director of a public company).

[56] *See, e.g.*, SEC v. Simmons, Litigation Release No. 19541, 2006 SEC LEXIS 145 (Jan. 24, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2006.shtml (noting the entry of an injunction against the defendants, permanently enjoining each of them from future violations of the registration, anti-fraud, and anti-touting provisions of the federal securities laws); SEC v. Wilson, Litigation Release No. 19092, 2005 U.S. Dist. LEXIS 12539 (Feb. 18, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (seeking an injunction prohibiting the defendant from trading in securities other than securities issued by registered open-end investment companies).

[57] *See, e.g.*, SEC v. Simmons, Litigation Release No. 19541, 2006 SEC LEXIS 145 (Jan. 24, 2005), *available at* http://www.sec.gov.litigation.litreleases/litrelarchive/litarchive2006.shtml (noting the imposition of a civil penalty of $400,000); SEC v. Invest Better 2001, Litigation Release No. 19221, 2005 SEC LEXIS 1043 (May 10, 2005), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2005.shtml (noting the imposition of a civil penalty of $1,237,371).

[58] *See, e.g.*, SEC v. Tuig, Litigation Release No. 19569, 2006 SEC LEXIS 372 (Feb. 17, 2006), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2006.shtml (noting the appointment of a receiver to deal with a company engaged in the sale of unregistered securities that netted the defendants $30 million); SEC v. Dowdell, Litigation Release No. 18198, 2003 SEC LEXIS 1469 (June 20, 2003), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2003.shtml (reporting on receiver's collection of more than $24 million for the benefit of investors).

[59] *See, e.g.*, SEC v. Weare, Litigation Release No. 17811, 2002 SEC LEXIS 2739 (Oct. 29, 2002), *available at* http://www.sec.gov/litigation/litreleases/litrelarchive/litarchive2002.shtml (ordering the defendants to disgorge over $6.2 million in funds obtained from investors).

fraud)[60] and the criminal history of the defendant (through which recidivists get appropriate credit for their criminal histories). Beyond these foundational items, however, there are provisions in the Guidelines for sentence enhancements that seem particularly well-suited to the circumstances of many online investment frauds. These provisions authorize sentence enhancements for the use of "mass-marketing," the involvement of multiple victims, the use of "sophisticated means" in perpetrating the crime, the use of "special skills," relocation from state-to-state or out of the United States in order to thwart detection of the crime, and significant use of offshore resources.[61] Sentence enhancements are also possible for the organizers or leaders of "extensive" fraud schemes.[62] And there is always the possibility of an upward departure to take into account aggravating factors not otherwise dealt with within the Guidelines.[63] Prosecutors also may seek restrictions on Internet access for defendants as a condition of probation or supervised release.[64]

A. *Use of "Mass-Marketing"*

The Federal Sentencing Guidelines provide for a two-level sentence enhancement where the crime "was committed through mass-marketing."[65] "Mass-marketing" is defined as "a plan, program, promotion, or campaign that is conducted through solicitation by telephone, mail, the Internet, or other means to induce a large number of persons to (i) purchase goods or services; (ii) participate in a contest or sweepstakes; or (iii) invest for financial profit."[66]

There should be little question that the "mass-marketing" enhancement should apply to online securities frauds conducted over the Internet, just as it does to non-securities related frauds conducted over the Internet.[67]

---

[60] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b).

[61] *See infra*, Sections A, B, C, D, E, and F.

[62] *See infra*, Section G.

[63] *See infra*, Section H.

[64] *See infra*, Section I.

[65] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(2)(A)(ii) (2004).

[66] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. 4(A).

B. High-Volume Victimization

The Sentencing Guidelines provide for a two-level sentence enhancement where the fraud involves ten or more victims.[68] Courts are authorized to enter a four-level enhancement where the fraud involves fifty or more victims.[69] Frauds involving 250 or more victims can result in a six-level enhancement.[70] These enhancements can easily be applied to widespread online securities frauds.[71]

C. "Sophisticated Means"

The Federal Sentencing Guidelines provide for a two-level sentence enhancement where the defendant's crime involved "sophisticated means."[72] To date, judges in reported federal court opinions have not found that the use of an interactive website itself constitutes "sophisticated means."[73] Reasoning by analogy, however, use of a website (or websites) in an online investment fraud should constitute "sophisticated if the creation of a website is now very simple.

---

[67] *See, e.g.*, United States v. Nickens, 38 F. App'x 721 (3d Cir. 2002) (affirming a two-level "mass-marketing" enhancement where defendant conducted an auction scam over the Internet); United States v. Blanchett, 41 F. App'x 181 (10th Cir. 2002) (holding the same); United States v. Pirello, 255 F.3d 728 (9th Cir. 2001) (affirming a two-level "mass-marketing" enhancement where defendant pleaded guilty to wire fraud in connection with the fraudulent sale of computer equipment over the Internet).

[68] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(2)(A)(i).

[69] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(2)(B).

[70] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(2)(C).

[71] *See, e.g.*, United States v. Stergios, 370 F. Supp. 2d 328 (D. Me. 2005) (applying a six-level enhancement where the defendant's fraud involved 321 victims).

[72] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9)(C). "For purposes of subsection (b)(9)(C), 'sophisticated means' means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means." *Id.* cmt. n.8.

[73] *See, e.g.*, United States v. Clark, 2004 FED App. 03-5624 (6th Cir.), 117 F. App'x 430. The opinion indicates that the United States Probation Office regards the use of a website alone as constituting a "sophisticated means." *Id.* at *432.

We know, for example, that the use of the Internet for communication and transmission of images, together with the use of a webcam, satisfies the "planning [and] sophistication" aggravating factor under California law.[74] So does the extraction of money from victims "by means of the Internet and the use of false identities."[75]

Certainly, an elaborate identity theft scheme in which the defendant gathers personal information on the Internet, and then, using that information, makes purchases in his victims' names by telephone, satisfies the "sophisticated means" requirement of federal law.[76]

I would argue that online investment frauds that use multiple websites, especially those involving purported links to phony analysts' reports and press releases, or posts purporting to come from multiple sources (and using multiple usernames) should satisfy the "sophisticated means" requirement. Just because the creation of a website (or multiple websites) is easy - many teenagers do it, and there are "build-a-website" instructions all over the Internet today[77]—does not negate the fact that many online investment schemes require the creation and maintenance of a complex set of sites and identities.

Certainly a Ponzi scheme, in which early investors are paid with the revenue received from investors arriving later, itself requires "sophisticated means," even where it does not involve the use of the Internet.[78]

---

[74] People v. Learn, No. A109084, 2005 Cal. App. LEXIS 11569, at *1 (Dec. 16, 2005).

[75] People v. Gaster, No. A104350, 2004 Cal. App. LEXIS 11340, at *1 (Dec. 16, 2004).

[76] United States v. Jackson, 346 F.3d 22 (2d Cir. 2003).

[77] *See, e.g.*, Build-Website.com, Build Your Own Website, http://www.build-website.com/ (last visited Jan. 14, 2007).

[78] United States v. Bistrup, 449 F.3d 873 (8th Cir. 2006).

D. Use of a "Special Skill"

The Federal Sentencing Guidelines authorize the imposition of a two-level enhancement where the defendant "used a special skill, in a manner that significantly facilitated the commission or concealment of the offense."[79] A "special skill" is defined as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing."[80]

Many courts agree that a defendant need not have had a *formal* education to qualify for a special skill enhancement.[81] Thus, a self-taught hacker who used his computer skills to retrieve personal data from the Internet in an identity-theft scheme was given a two-level "special skills" enhancement.[82] A disgruntled ex-employee who used his knowledge of his employer's computer system to enter the site and destroy valuable data was given a two-level sentence enhancement because he had skills "beyond those possessed by an ordinary computer user."[83] The Court of Appeals said nothing about whether his scheme required formal education.

Some courts, however, are reluctant to impose a "special skill" enhancement on defendants who used their computer skills to engage in online fraud, primarily because those skills do not require formal education. Thus, a clever programmer who created a "mirror" website for the Honolulu Marathon in Japanese, rather than English, and who then misappropriated registration fees from Japanese runners, was found ineligible for a "special skills" enhancement because his computer skills were not "particularly sophisticated."[84] Likewise, a defendant who used his computer skills to produce counterfeit bills on

---

[79] U.S. SENTENCING GUIDELINES MANUAL § 3B1.3 (2005).

[80] *Id.* cmt. n.4.

[81] United States v. Prochner , 417 F.3d 54, 61 (1st Cir. 2005).

[82] *Id.* at 62; *see also* United States v. Petersen, 98 F.3d 502 (9th Cir. 1996) (hacker given a two-level enhancement, although he had had no formal training on computers).

[83] United States v. O'Brien, 435 F.3d 36, 42 (1st Cir. 2006).

[84] United States v. Lee, 296 F.3d 792 (9th Cir. 2002) (overturning enhancement).

Adobe Page Maker was also found not to be eligible for a "special skills" enhancement.[85]

It would be useful, of course, to have a little more guidance from the courts on just how much "sophistication" is required of computer-based schemes for the "special skills" enhancement to be appropriate. We do know, however, that the "sophisticated means" enhancement and the "special skills" enhancement are not identical (and, therefore, are not mutually exclusive).[86] So the question of "sophistication" may not really be the right one to ask on the issue of whether the defendant employed special skills. Rather, the question should be whether an "ordinary" computer user would be able to fashion the type of website or interactive program necessary to execute a particular securities fraud scheme.

E. *Relocating to Avoid Detection*

The Federal Sentencing Guidelines authorize the trial courts to impose a two-level sentence enhancement where the defendant "relocated, or participated in relocating, a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials."[87] This provision encompasses a defendant's relocation from state to state, as well as relocation outside of the United States.[88] Many securities law violators have a history of moving from state to state and taking their schemes with them. A relocation enhancement might well be appropriate for defendants in this category. One might also argue that a securities law violator that moves from website to website or from server to server should also be eligible for a "relocation" enhancement.

---

[85] United States v. Godman, 223 F.3d 320 (6th Cir. 2000) (overturning enhancement).

[86] United States v. Olis, 429 F.3d 540, 549 (5th Cir. 2005); United States v. Minneman, 143 F.3d 274, 283 (7th Cir. 1998) ("The special skill adjustment focuses on [the defendant's] use of his [professional] training. The sophisticated means enhancer arises because of the use of multiple accounts and corporate names. Thus, both enhancements could be invoked.").

[87] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9)(A) (2005).

[88] United States v. Stokes, 75 F. App'x 888 (3d Cir. 2003).

F. Use of an Offshore Location

The Federal Sentencing Guidelines authorize the trial court to impose a two-level sentence enhancement where "a substantial part of a fraudulent scheme was committed from outside the United States."[89] Many securities fraud schemes are now orchestrated from outside the United States, raising significant enforcement problems.[90] To the extent that the government is able to bring the perpetrators of these schemes to justice in the United States, this two-level enhancement is custom-built just for them.

G. Aggravating Role

The Federal Sentencing Guidelines authorize the imposition of a three- or four-level enhancement where the scheme involves five or more participants, and the defendant served as the "organizer or leader," or "manager or supervisor" of the scheme.[91] An "organizer or leader" is more culpable than a "manager or supervisor" and thus is subject to an extra one-level enhancement. This set of enhancements also takes into account the existence of unwitting accomplices.[92]

These provisions will have no application to a con artist who single-handedly, creates a website and handles all of the postings and communications involved in executing an online investment scheme. However, schemes involving five or more actors invite the application of one of these "role" enhancements.[93]

---

[89] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(9)(B).

[90] *See, e.g.*, Burke v. China Aviation Oil Corp., Exchange Act Release No. 05 Civ. 0060 [2005-2006 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 93,621 (Nov. 29, 2005) (dismissing action against an issuer that sold its securities from an offshore website for lack of subject matter jurisdiction).

[91] U.S. SENTENCING GUIDELINES MANUAL § 3B1.1.

[92] *Id.* cmt. n.3 (construing the term "otherwise extensive" as including unknowing outsiders).

[93] *See, e.g.*, United States v. Aptt, 354 F.3d 1269, 1285 (10th Cir. 2004) (affirming a four-level "organizer or leader" enhancement for a defendant who orchestrated a Ponzi scheme).

H. Upward Departures for Crimes "Outside the Heartland"

The Federal Sentencing Guidelines provide for departures from the calculated sentence where the court finds "an aggravating or mitigating circumstance . . . not adequately taken into consideration by the Sentencing Commission in formulating the guidelines."[94] Departures are typically applied to sentences imposed for crimes that are said to be "outside the heartland" of the "typical" crimes around which the Sentencing Guidelines were formulated.[95]

An upward departure in a fraud case may be appropriate where the defendant is a recidivist, his misconduct extends over a period of years and across several states, and reaches victims all over the United States.[96] It may also be appropriate where the scheme is extensive both in terms of the amount of money extracted and the number of victims ensnared, especially where the result is that "thousands of investors lost their life savings."[97] Courts may focus on the fact that victims have lost "irreplaceable" funds and have been unable to meet their financial obligations.[98]

I. Limitations on Access to the Internet as a Condition for Probation or Supervised Release

There is one final tool available to prosecutors, in addition to sentence enhancements and upward departures. Federal and state courts often impose conditions on a sentence of probation or supervised release, including limitations on computer or Internet usage. While a complete ban on Internet access may be appropriate in some cases (typically involving defendants convicted of the online sale of child pornography),[99] limitations on access must be reasonably related to the defendant's rehabilitation and protection of the public.[100]

---

[94] 18 U.S.C. § 3553(b) (2000).

[95] Koon v. United States, 518 U.S. 81, 105 (1996).

[96] United States v. Passmore, 984 F.2d 933, 938 (8th Cir. 1993) (affirming upward departure).

[97] United States v. Stouffer, 986 F.2d 916, 928 (5th Cir. 1993) (affirming upward departure).

[98] United States v. Scrivener, 189 F.3d 944, 951 (9th Cir. 1999) (affirming a two-level upward departure).

[99] *See, e.g.*, United States v. Fields, 324 F.3d 1025, 1027 (8th Cir. 2003).

Within this boundary, federal courts have limited Internet access in a number of specific ways. For example, one defendant with a history of identity theft was permitted to use the Internet at work, "so long as he ha[d] no access to personal information including bank account numbers, credit card numbers, social security numbers and birth dates."[101] Another defendant was prohibited from accessing any Internet bulletin boards unless specifically approved by the U.S. Probation Office.[102]

Defendants permitted *some* access to computers may, as a condition of supervised release, be denied access to certain types of hardware or software consistent with their criminal history.[103] Their access to a computer may also be conditioned upon installation of a monitoring application, such as a keystroke-reading program, and subject to random monitoring by the U.S. Probation Office.[104]

State courts have also imposed restrictions on access to the Internet in some cases. These kinds of restrictions are common for sex offenders whose crimes involved Internet communications or file transfers.[105] Courts have also imposed Internet access limitations on defendants found guilty of identity theft.[106] Certainly, defendants who have exploited the quick and cheap communications capacity of the Internet to commit investment fraud, especially those who have created phony analyst reports, news sites, or multiple identities to advance their schemes, can reasonably expect to be restricted in their access to the Internet, at least for the duration of their supervised release.

---

[100] *See* United States v. Crume, 422 F.3d 728, 732 (8th Cir. 2005) (articulating the limitations that govern conditions of probation or supervised release); United States v. Scott, 316 F.3d 733, 735 (7th Cir. 2003) (cautioning against too aggressive use of restrictions on Internet access as a condition of probation or supervised release).

[101] United States v. Stanfield, 360 F.3d 1346, 1352 (D.C. Cir. 2004) (remanding case for clarification of the scope of the restriction).

[102] United States v. Crandon, 173 F.3d 122, 128 (3rd Cir. 1999).

[103] *See, e.g.*, United States v. Goba, 220 F. Supp. 2d 182 (W.D.N.Y. 2002). The defendant was not allowed to possess, purchase, or use a computer that included a modem, Internet account, writable or rewritable CD Rom, tape backup or removable mass storage device. *Id.* at 195. "If allowed use of a computer for employment, the system [could] only contain software required to perform his job." *Id.* at 196.

[104] *See, e.g.*, United States v. Liu, No. 03 Cr.782 (LTS), 2006 U.S. Dist. LEXIS 13849, at *3-16 (S.D.N.Y. Mar. 29, 2006) (detailing the conditions imposed on the defendant by the U.S. Probation Office at and after sentencing); *but see* United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004) (remanding for consideration of the details of the government's proposed computer-monitoring program, to ensure that it is not overly burdensome).

III. NEW TOOLS TO ADDRESS ONLINE INVESTMENT FRAUD

What I have described up until this point tries to capture what is likely to happen in the prosecution of online investment fraud. The fact is, there are few reported cases in this area—and there are good reasons for that. First, since the unfolding of the Enron, WorldCom, and other spectacular financial reporting crimes in 2001 and 2002, many SEC lawyers and financially-sophisticated lawyers at the Department of Justice have been assigned to those high profile cases.[107] Second, prosecuting online investment schemes requires two sets of valuable skills: an understanding of the technology and an understanding of the securities laws. People with both of these skills are valuable outside of government and get recruited away. Third, where the Department of Justice has to prioritize its workload, cybercrimes involving pornography or infrastructure attacks are likely to receive more attention than the ones involving investment schemes.

Still, using the tools at hand, the Department of Justice has generated a significant record in crafting tough sentences for defendants convicted of online investment fraud.[108] In this section of the Article, I want to propose three additional tools that would aid in appropriate sentencing of these defendants. I will also propose an additional device: a public registry designed to deter recidivist offenders.

---

[105] *See, e.g.*, People v. Harrisson, 36 Cal. Rptr. 3d 264, 271 (2005) (affirming order prohibiting Internet access as a condition of probation); People v. Crumpler, No. E035407, 2005 Cal. App. LEXIS 1594, at *9 (Feb. 24, 2005) (same).

[106] *See, e.g.*, People v Malone, No. C042537, 2003 Cal. App. LEXIS 7603, at *11 (Aug. 5, 2003) (affirming order prohibiting use of e-mail, internet, scanners, or digital cameras).

[107] Deborah Solomon, *Executives on Trial: Crackdown Puts Corporations, Executives in New Legal Peril*, WALL ST. J., June 20, 2005, at A1. Since the formation of the corporate fraud task force in 2002, the Justice Department has charged more than 900 individuals in more than 400 cases. *Id.*

A. Authorize an Enhancement for Use of a Computer in Perpetrating a Fraud

Let us assume that the use of an interactive website, without more, does not qualify for a "sophisticated means" enhancement. Although I have argued above that it should qualify, there is a plausible argument that it does not. I propose that the Sentencing Guidelines be amended to provide clearly for the availability of a two-level enhancement whenever the Internet is an indispensable element of a federal fraud, securities, or otherwise.

There is already a template for a provision like this. The Sentencing Guidelines already authorize a two-level enhancement if the offense involves a violation of the Computer Fraud and Abuse Act with an "intent to obtain personal information."[109] A similar provision could authorize a two-level enhancement if the offense involves the use of the Internet with an intent to obtain money or other items of value by unlawful means.

To support such a provision, I would offer two possible arguments: first, use of the Internet to effectuate a fraud is, in effect, a home invasion; second, use of the Internet to effectuate a fraud is similar to using a gun in a crime—it increases exponentially the likelihood that harm will occur.

---

[108] *See, e.g.*, SEC v. New Energy Corp., Litigation Release No. 19670, 2006 SEC LEXIS 952 (Apr. 26, 2006), *available at* http://www.sec.gov/litigation/litreleases/2006/lr19670.htm (noting that participants in an Internet-based "pump and dump" scheme had been sentenced to nine-year, six-year, and three-month prison sentences, respectively); SEC v. Tri-West Inv. Club, Litigation Release No. 19267, 2005 SEC LEXIS 1407 (June 14, 2005), *available at* http://www.sec.gov/litigation/litreleases/lr19267.htm) (noting that the defendant had been sentenced to 120 months in connection with an Internet-based investment fraud scheme); SEC v. Roor, Litigation Release No. 18876, 2004 SEC LEXIS 2134 (Sept. 9, 2004), *available at* http://www.sec.gov/litigation/litreleases/lr18876.htm (noting that the defendants had been sentenced to sixty, forty-six, thirty-three, and thirty months respectively for their role in Internet-based "risk-free" investment schemes).

[109] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(14)(A)(i)(II) (2005).

B. Authorize an Upward Departure for Online Crimes Against the Elderly

Thirteen years ago, Congress recognized the especially pernicious use of telemarketing techniques to prey on elderly, often lonely, victims. The Senior Citizens Against Marketing Scams (or SCAMS) Act provides for a significant upward departure where a telemarketing scheme either victimizes ten or more persons over the age of fifty-five[110] or targets persons over the age of fifty-five.[111]

Today's fraud schemes have taken technology one step further. Rather than relying on costly telemarketing campaigns, promoters now often rely on the use of interactive websites, aided by e-mail communication. Telephone follow-up may or may not be involved in these schemes. Still, the Internet approach operates very much like telemarketing. It permits the promoter to enter the victim's home, slowly build a sense of trust and confidentiality, and then time communications to maximize the likelihood of the victim making an investment decision. It would certainly make sense, at a minimum, to amend the SCAMS Act to incorporate spam e-mail campaigns.

C. Authorize an Enhancement for Investments Made With Funds from a Retirement Account

Oftentimes victims move money from safe into unsafe investments because of the lure of a fraud scheme.[112] It should matter for purposes of sentencing where the victim's money came from. The State of Utah recognized this when it distinguished, as a matter of substantive law, between investment schemes generally, and those that involve the receipt of money from any of the following sources: equity in a person's home, a withdrawal from any individual retirement account, or a withdrawal from any qualified retirement plan.[113] The Sentencing Guidelines should be amended to provide for a two-level sentence enhancement where victims' losses are traceable to a decision to cash in equity in their home, make a withdrawal from an IRA, or make a withdrawal from any qualified retirement plan.

---

[110] 18 U.S.C. § 2326(2)(A) (2000).

[111] *Id.* § 2326(2)(B).

[112] *See, e.g.*, SEC v. Richmond, Litigation Release No. 17609, 2002 SEC LEXIS 1773 (July 12, 2002), *available at* http://www.sec.gov/litigation/litreleases/lr17609.htm (describing Internet-based Ponzi scheme, in which sales agents "convince[d] unsophisticated investors, including many elderly persons and widows, to

D. Register Securities Law Violators

A final recommendation derives from what we already do with respect to sexual predators and physicians with a history of malpractice or disciplinary complaints: compile a registry and put the public on notice of their history and conduct. Currently, there is no one place for prospective investors to go to check on the bona fides of a person in whose business they are contemplating an investment. A Google search may develop some information about previous stock frauds or other misconduct, but there is no central repository for this information, either at the state or federal level.

One might argue that it is easy for defendants to change their names, or the names of their companies, and that any registry would be imperfect, perhaps misleading. Certainly, name changes and multiple websites are not uncommon. Still, the cost of creating a registry is small, and the existence of a registry, like the existence of "watch out" websites that warn potential investors of the risks of online investments,[114] can

---

liquidate annuities and other investments in order to purchase fraudulent securities").

[113] UTAH CODE ANN. § 61-1-21 (2005). Thanks to Richard Hamp, Assistant Attorney General in Utah, for directing me to this provision.

[114] *See* Lynn Cowan, *Investor Education 101: How to Avoid Scams*, WALL ST. J., May 9, 2006, at D3 (noting the SEC's creation of cautionary websites that pose as "can't fail" investment schemes: when the surfer clicks through to the

only serve as an additional deterrent, both to perpetrators of fraud and to their eager victims.

IV. CONCLUSION

Not long ago, a critic of the Securities and Exchange Commission advocated ratcheting up the criminal enforcement of the securities laws, especially violations involving "boiler rooms, pump and dump schemes, and [the sale of] outright fraudulent securities."[115] Others have suggested that securities law violators—especially recidivist securities law violators—simply are not deterred by the imposition of civil sanctions.[116]

One need not abandon civil sanctions before seeking an optimum strategy for criminal enforcement. In this Article, I have set out a number of the tools that are available to prosecutors of online investment fraud. I have also set out four additional tools that would give criminal enforcement of the securities laws even sharper teeth.

"tell me more" screen, they are told, "STOP—this is a scam").

[115] Thad A. Davis, *A New Model of Securities Law Enforcement*, 32 CUMB. L. REV. 69, 92 (2001-2002).

[116] Richard H. Walker & David M. Levine, *"You've Got Jail": Current Trends in Civil and Criminal Enforcement of Internet Securities Fraud*, 38 AM. CRIM. L. REV. 405 (2001).

Mitchell
McNutt
& Sams

Attorneys at Law

www.mitchellmcnutt.com

Raise the bar.

Bradley Arant Rose & White LLP is pleased to announce that 78 of our partners are recognized in the 2007 edition of *The Best Lawyers in America*.

We call that raising the bar.

Bradley Arant
BRADLEY ARANT ROSE & WHITE LLP

BIRMINGHAM CHARLOTTE HUNTSVILLE JACKSON MONTGOMERY WASHINGTON, DC *www.bradleyarant.com*

FEDERAL AND
STATE CRIMINAL DEFENSE

FELLOW - ABCL
LIFE MEMBER - NACDL

John M. Colette

Attorney at Law

TELEPHONE (601) 355-6277
FAX (601) 355-6283
TOLL-FREE 888-659-6277

401 EAST CAPITAL STREET, SUITE 308
P.O. BOX 861
JACKSON, MISSISSIPPI 39205

O&G

OWEN AND GALLOWAY
ATTORNEYS AT LAW

Owen Building
1414 25th Avenue
Post Office Drawer 420
Gulfport, MS 39502-0420
Telephone: 228-868-2821
Fax: 228-864-6421 or 228-868-2813
e-mail: ogc@owen-galloway.com
website: www.owen-galloway.com

FORMAN
PERRY
WATKINS
KRUTZ &
TARDY LLP

ATTORNEYS AT LAW

Dallas • Houston • Jackson • New Orleans

Some law firms want it. Butler Snow has IT.

At Butler Snow, we adapt advances in information technology to enhance client service. Ken Jones, our Director of IT, was named one of the Top 100 Global Tech Leaders by *Citytech*, an industry newsletter.* Staying on the leading edge of law and technology helps Butler Snow rank as one of America's Top 100 law firms, according to a survey by BTI Consulting Group of *Fortune 1000*™ companies.† When you put clients first, they notice.

BUTLER SNOW
BUTLER, SNOW, O'MARA, STEVENS & CANNADA, PLLC

ATTORNEYS AT LAW

Jackson, MS 601-948-5711 Gulfport, MS 228-864-1170 Memphis, TN 901-680-7200

butlersnow.com

** Based on a survey of more than 2,000 global technologists from law firms, vendors, the press and consulting firms.*
† Based on independent interviews with general counsels and key decision-makers who hire law firms.

FREE BACKGROUND INFORMATION AVAILABLE UPON REQUEST.

National Center for Justice and the Rule of Law

The University of Mississippi School of Law

The National Center for Justice and the Rule of Law is a part of the University of Mississippi School of Law. The Center focuses on issues relating to the criminal justice system, with its purpose to promote the two concepts comprising the title of the Center. The concept of "justice" appeals to basic notions of equality, equity, and fairness, often with an emotive component. In contrast, the phrase "rule of law" refers to the requirement that certain procedures and principles must be followed in each case to reach a correct result. Neither concept is sufficient; rather, both must be utilized to ensure that the criminal justice system fulfills its function in society. The Center implements its mission through projects, conferences, educational programs, and publications that examine important criminal law and procedural issues.

Thomas K. Clancy
Director

The Center has five programs:

National Programs Initiative

Helps state governments investigate sophisticated criminal activity through training and model programs designed to attack computer-related crime.

Fourth Amendment Initiative

Promotes awareness of search and seizure principles through conferences, training, and support for selected publications.

Prosecution Externship Program

Provides specialized course-work and real-world training for law students in the duties and responsibilities of prosecutors.

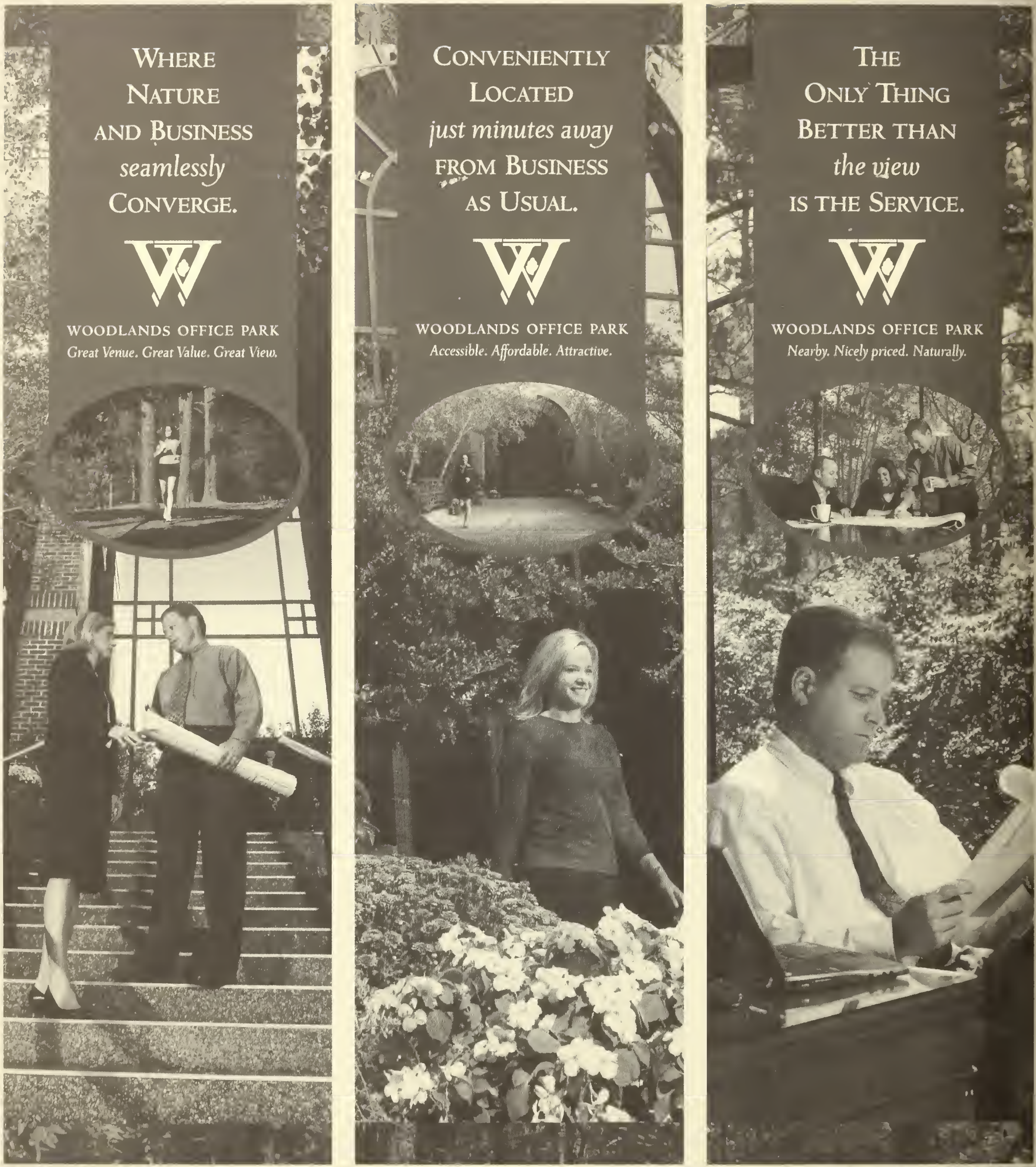
Criminal Appeals Clinic

Provides law students with intensive training representing on appeal persons convicted of crimes.

Special Projects

Provides support for selected projects that promote the concepts of justice and the rule of law.

Visit the Center's website at www.NCJRL.org for additional information about these programs.


WHERE NATURE AND BUSINESS *seamlessly* CONVERGE.
W
WOODLANDS OFFICE PARK
Great Venue. Great Value. Great View.
CONVENIENTLY LOCATED *just minutes away* FROM BUSINESS AS USUAL.
W
WOODLANDS OFFICE PARK
Accessible. Affordable. Attractive.
THE ONLY THING BETTER THAN *the view* IS THE SERVICE.
W
WOODLANDS OFFICE PARK
Nearby. Nicely priced. Naturally.

WOODLANDS OFFICE PARK
RIDGELAND, MISSISSIPPI

For leasing information on the Woodlands contact:
Woodlands Realty Group, LLC
Russell Wilcox, *Broker*
(601) 956-9833
www.woodlandsrealtygroup.com • **E-mail:** rwilcox@woodlandsrealtygroup.com